HiPER ReOS 6.0

VPN 配置手册

上 海 艾 泰 科 技 有 限 公 司

http://www.utt.com.cn

版权声明

本文档所提供的资料包括 URL 及其他 Internet Web 站点参考在内的所有信息，如有变更，恕不另行通知。

除非另有注明，本文档中所描述的公司、组织、个人及事件的事例均属虚构，与真实的公司、组织、个人及事件无任何关系。

本手册及软件产品受最终用户许可协议（EULA）中所描述的条款和条件约束，该协议位于产品文档资料及软件产品的联机文档资料中，使用本产品，表明您已经阅读并接受了 EULA 中的相关条款。

遵守所生效的版权法是用户的责任。在未经上海艾泰科技有限公司明确书面许可的情况下，不得对本文档的任何部分进行复制、将其保存于或引进检索系统；不得以任何形式或任何方式（电子、机械、影印、录制或其他可能的方式）进行商品传播或用于任何商业、赢利目的。

上海艾泰科技有限公司拥有本文档所涉及主题的专利、专利申请、商标、商标申请、版权及其他知识产权。在未经艾泰科技有限公司明确书面许可的情况下，使用本文档资料并不表示您有使用有关专利、商标、版权或其他知识产权的特许。

艾泰®、UTT®文字及相关图形是上海艾泰科技有限公司的注册商标。

HiPER®文字及其相关图形是上海艾泰科技有限公司的注册商标。

此处所涉及的其它公司、组织或个人的产品、商标、专利，除非特别声明，归各自所有人所有。

产品编号（PN）：0900-0059-001

文档编号（DN）：PR-PMMU-1107.06-PPR-CN-1.0A

目 录

第1章 HiPER VPN 解决方案

随着 Internet 和 Intranet 技术的发展，虚拟专用网 VPN 技术以其管理简单、费用低廉的优点成为企业构建内部网络的首要选择。

本章主要介绍了 VPN 的主要技术、HiPER VPN 网关产品以及应用方案。

1.1 缩略语与专用名词

VPN（Vitual Private Network），虚拟专用网：VPN 指的是依靠 ISP（Internet Service Provider 因特网服务提供商）和其它 NSP（Network Service Provider 网络服务提供商），在公用网络（如 Internet）中建立专用的数据通信网络的技术。

PPTP（Point-to-Point Tunneling Protocol），点到点隧道协议：PPTP 是一种虚拟专用网络协议，属于第二层的协议。PPTP 将 PPP（Point-to-Point Protocol）帧封装在 IP 数据报中，通过 IP 网络如 Internet 或企业专用 Intranet 等发送。

L2TP（Layer Two Tunneling Protocol），第二层隧道协议：L2TP 是一种虚拟专用网络协议，已成为 IETF 有关二层隧道协议的工业标准。L2TP 将 PPP（Point-to-Point Protocol）帧封装后，可通过 IP，X.25，帧中继或 ATM 等网络进行传送。

IPSec（IP Security Protocol），IP 网络安全协议：IPSec 是 IETF 制定的一系列协议，以保证在 Internet 上传送数据的安全保密性能，通信方之间在 IP 层通过加密与数据源验证来保证数据包在 Internet 上传输时的私有性、完整性和真实性。

IETF（Internet Engineering Task Force），因特网工程任务组：全球因特网组织中专门负责开发因特网协议的组织之一。IETF 的工作是围绕着若干工作小组展开的，每个小组专门负责某一类问题或某一类协议的研究制定。

RFC（Request for Comment），请求注释文档：IETF 设计的文档编制机制，用于提供 Internet 各个组成部分的实现标准。任何实现（协议或通信方法），都可以通过文档的形式提交给 IETF。IETF 分析文档后，就赋予该文档一个惟一的编号，然后公开发布该 RFC 文档。

1.2 VPN 的主要技术

虚拟专用网(VPN)主要采用了两种技术：隧道技术与安全技术。隧道技术当前主要有三种协议支持：PPTP，L2TP和IPSec。安全技术主要有IPSec等。

VPN具体实现是采用隧道技术，将数据包封装在隧道中进行传输。隧道协议可分为第二、第三层隧道协议。第二层隧道协议（如PPTP、L2TP）是先把各种网络协议封装到PPP帧中，再把整个数据包装入隧道协议中。这种双层封装方法形成的数据包靠第二层协议进行传输。第三层隧道协议（如IPSec、GRE等）是先把各种网络协议直接装入隧道协议中，形成的数据包依靠第三层协议进行传输。

为了保证传输的安全，需要一定的安全加密手段保证数据的私密性和完整性。虽然PPTP和L2TP各自有自己的优点，但是都没能很好地解决隧道加密和数据加密的问题。而IPSec协议支持对数据加密，同时确保数据的完整性。IPSec为IP网络通信提供透明的安全服务，保护TCP/IP通信免遭窃听和篡改，可以有效抵御网络攻击。IPSec提供两种安全机制：加密和认证。认证机制使IP通信的数据接收方能够确认数据发送方的真实身份以及数据在传输过程中是否遭篡改。加密机制通过对数据进行编码来保证数据的机密性，以防数据在传输过程中被窃听。

PPTP/L2TP 提供了能够满足大多数公司需要的安全性级别，同基于 IPSec 的 VPN 解决方案相比，它们使用的安全模型虽然不够完整但是仍然具有一些优点，如容易使用，部署方便等。尽管 IPSec 具有更高的安全性和可靠性，但是它的部署通常更加复杂，而且受到一定的限制，如有些 NAT 设备不支持 IPSec 数据穿透等。因此，在实际应用中，应该根据实际需求选择相应的方式。

使用 Windows 2000 或 Windows XP 客户机本身都能够充当 PPTP/L2TP VPN 客户机，因此 VPN 通道可以直接扩展到拨号用户的计算机上，从而提供端对端通道。另外，Microsoft 公司在新版本的 Windows 软件中（Windows XP）提供了初步的 IPSec VPN 支持。

1.3 HiPER VPN 解决方案

使用 HiPER 虚拟专用网（VPN）解决方案，可以通过公共网络为企业在公司总部与各远程分支机构以及移动商务人员之间提供一个安全的网络连接。服务提供商还可以使用 HiPER 虚拟专用网（VPN）解决方案为他们的客户提供 VPN 服务。

1.3.1 HiPER VPN 网关

HiPER 是上海艾泰科技有限公司开发的新一代集成的 VPN 网关，HiPER 产品的 VPN 功能支持 PPTP，L2TP 和 IPSec 三种 VPN 协议，为用户提供了前所未有的方便和灵活的选择。

对于远程移动用户或其他出差用户来说，既可以使用 Windows 系统内置的 PPTP/L2TP 拨号软件，也可以使用 IPSec 客户端软件同企业建立 VPN 的连接。使用 PPTP、L2TP 的好处是方便，不需要另外的软件；而使用 IPSec 客户端软件的好处是更高的安全性和可靠性保证。

对于公司总部和各远程分支机构而言，使用 HiPER VPN 网关的好处是高度的安全性保证，可以通过采用动态的密钥来保证数据的安全。在企业本地网络和远程网络之间可以采用 IPSec 协议来建立 VPN 的连接，从而保证数据的机密性、可靠性和真实性。

HiPER VPN 网关提供友好的人性化的 WEB 管理界面，方便使用和管理。即使用户没有丰富的网络知识，也可以很快掌握配置和维护 HiPER VPN 网关的方法，为企业充分利用 VPN 技术快速构建其 Intranet 网络提供了保证。

HiPER VPN 网关的特点包括：

1. 集成的解决方案，提供全面的 VPN 功能， 同时支持 IPSec、L2TP 及 PPTP VPN。
2. 符合行业标准，通过 ICSA 认证。

1) 在隧道模式下的 IPSec 协议
2) DES，3DES 和 AES 加密
3) HMAC MD5 和 HMAC SHA-1 数据完整性认证
4) 基于预共享密钥的 IKE
5) 手动密钥通道
6) Diffie-Hellman 组 1、2、和 5
7) 野蛮模式和主模式
8) 抗重播
9) 前向保密（需要软件升级）

3. L2TP VPN 标准。
   1) L2TP 服务器
   2) L2TP 客户端
   3) 基于 L2TP 的远程拨号的 VPN
   4) 基于 L2TP 的 LAN 到 LAN 的 VPN
4. PPTP VPN 标准。
   1) PPTP 服务器
   2) PPTP 客户端
   3) 基于 PPTP 的远程拨号的 VPN
   4) 基于 PPTP 的 LAN 到 LAN 的 VPN
5. 基于防火墙策略的 IPSec VPN。
6. IPSec NAT 穿透技术，允许位于 NAT 后面的远程 IPSec VPN 网关或 VPN 客户端连接到 IPSec VPN 网关。
7. VPN 星形连接，可以使 VPN 流量从一个隧道经 HiPER 连接到另一个隧道。
8. IPSec VPN、L2TP VPN 或 PPTP VPN 与 DDNS 相结合，可实现无固定 IP 地址的 VPN。

1.3.2 HiPER VPN 应用

1.3.2.1 企业 Intranet 应用

企业 Intranet 网络建设的 VPN 连接方案利用 IPSec 安全协议的 VPN 和加密能力，实现两个或多个企业分支机构之间跨越 Internet 的企业内部网络连接，实现了安全的企业内部数据通信。通过 HiPER 内部策略控制体系对 VPN 的数据可以进行有效的控制和管理，使企业的内部网络通信具有良好的扩展性和管理性。

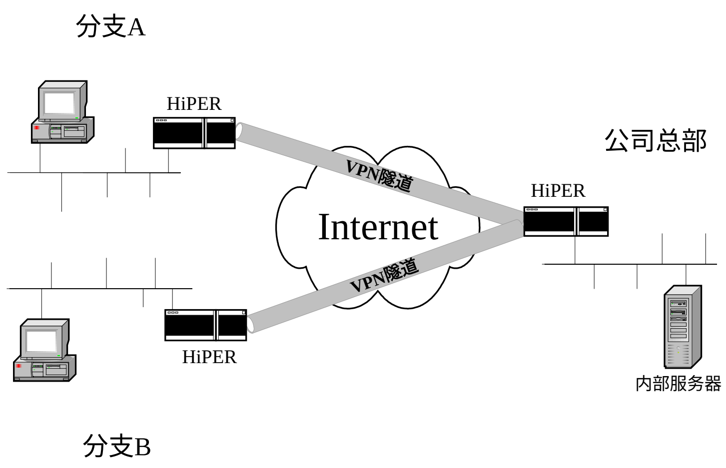


图 1-1 企业 Intranet VPN 应用

1.3.2.2 企业移动办公 VPN 应用

对于移动的办公室、出差用户、及采用 ADSL 上网的分支办公室，HiPER VPN 网关都提供了完善的解决方案。HiPER 支持 PPTP/L2TP/IPSec 多种协议体系，而且对于用户来说，其配置和使用都非常方便。如图 1-2，给出了分支办公室动态地址方式、移动办公用户、出差用户和总部中心的 VPN 连接解决方案。

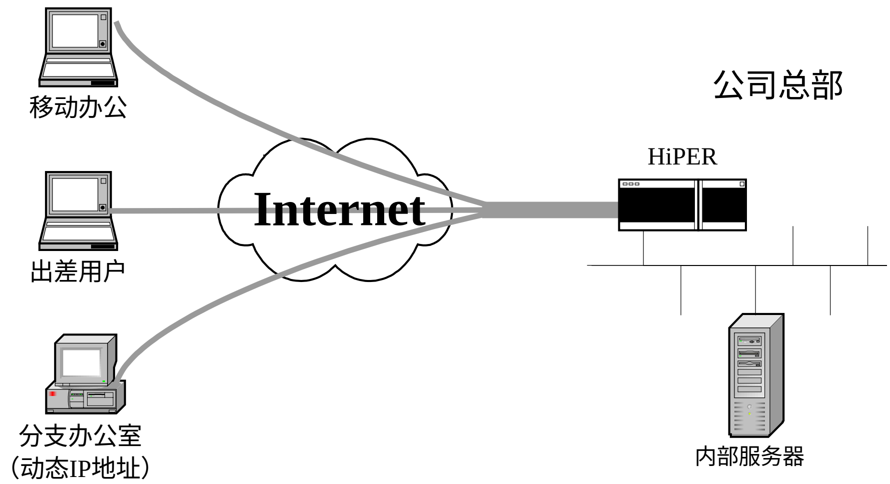


图 1-2 企业移动办公 VPN 应用

1.3.2.3 NAT 情况下的 VPN 应用

HiPER VPN 网关同时还设计了一项简单易用的 VPN Pass-Through 功能，称为 VPN 透明通过技术。使得 HiPER 在 NAT 情况下，保证远程 VPN 管理的正常应用。在很多企业中，企业总部需要对分支企业或分部进行统一的远程安全管理。为了保证管理数据的安全和私密性，利用远程 VPN 管理是理想的方式。但如果管理中心主机是通过 NAT 转换后建立 VPN 的话，PPTP、IPSec 协议不能成功建立。如果选用 HiPER 产品作为企业的 NAT 设备，则能透明地转发 PPTP/IPSec VPN 数据包，保证企业远程管理的正常应用。

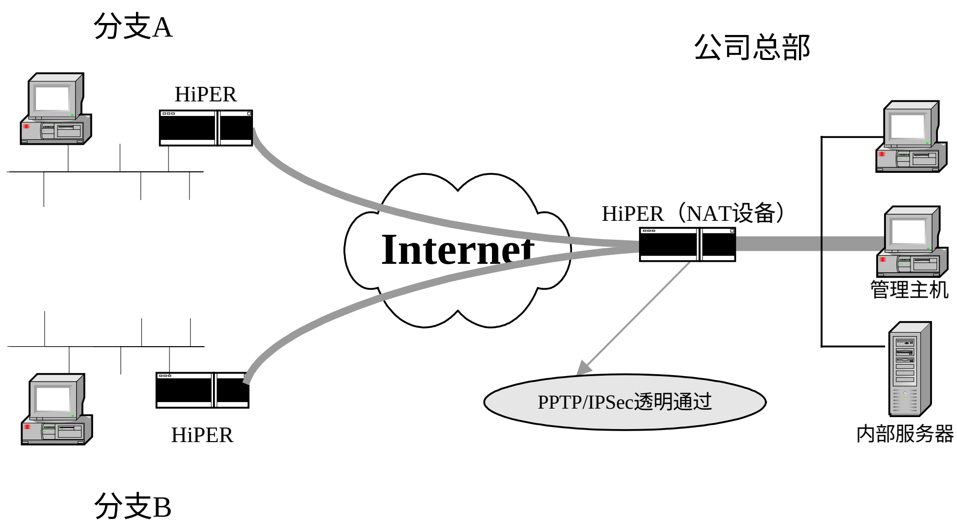


图 1-3 VPN 透明通过解决方案

在 HiPER 的 VPN 设计中，可以支持双向的 NAT 处理，使远程办公室的主机以本地 IP 地址的方式出现，增强了网络兼容性。VPN 的策略控制设计，使管理员可以灵活控制使用 VPN 隧道的 IP 地址、服务、时间等参数，增强了 VPN 安全控制。

作为新一代的安全网关设备，HiPER 以其贴近未来应用的设计理念将领导 VPN 网关产品市场的新变革。

1.4 小结

对企业来说，虚拟专用网 (VPN) 是一种具有成本效益的安全方法。HiPER VPN 设备是在多个企业网络中提供安全 VPN 访问的最佳选择。根据用户规模的大小，连接到 HiPER VPN 设备的用户可以使用 VPN 客户端软件或者 HiPER VPN 网关。例如，小型的办公室可以使用 HiPER 3100VF 或 3300VF，分支办公机构可以使用 HiPER 3300VF 或 HiPER 4520VF。服务供应商还可以用 HiPER 4520VF 或 3300VF 为多个客户网络提供 VPN 服务，每个网络连接到一个不同的用户定义接口。

第2章 HiPER 中 L2TP 的实现

L2TP 协议是一种虚拟专用网协议（VPN），该协议可以完成 PPP 封装的数据包在 IP 网络上的传送，L2TP 协议工作在客户机/服务器（Client/Server） 模式下，通信的双方拨出（发起呼叫）的一方叫客户端（Client），拨入（接受呼叫）的一方叫服务器（Server）。使用 L2TP 协议可以在 IP 网（如宽带网）中提供类似于拨号网络（如电话线）的远程接入服务，扩展企业网的范围，实现 VPN 应用。

本章描述了 L2TP 协议在 HiPER VPN 网关中的实现，包括如下内容：

缩略语与专用名词（章节 2.1）

L2TP 实现概述（章节 2.2）

L2TP 会话数量限制（章节 2.3）

小结（章节 2.4）

协议标准及参考资料（章节 2.5）

2.1 缩略语与专用名词

L2TP（Layer Two Tunneling Protocol），第二层隧道协议：L2TP 是一种虚拟专用网络协议，已成为 IETF 有关二层隧道协议的工业标准。L2TP 将 PPP（Point-to-Point Protocol）帧封装后，可通过 IP，X.25，帧中继或 ATM 等网络进行传送。

LAC（L2TP Access Concentrator），L2TP 访问集中器：LAC 作为 L2TP 隧道的一侧端点，是 LNS 的对端设备。LAC 在 LNS 和远端系统之间传递信息包，将从远端系统收到的信息包按照 L2TP 协议进行封装并送往 LNS，将从 LNS 收到的信息包进行解封装并送往远端系统。

LNS（L2TP Network Server），L2TP 网络服务器：LNS 作为 L2TP 隧道的另一侧端点，是 LAC 的对端设备，是被 LAC 进行隧道传输的 PPP 会话的逻辑终止端点。

PPP（Point-to-Point Protocol），点对点协议：PPP 协议是为在两点之间传输数据包的简单链路设计的，这些链路提供全双工的同时双向操作，而且按顺序传送数据包。

MTU（Maximum Transmission Unit），最大发送单元：物理端口可以发送的最大数据包长度。

MRU（Maximum Receive Unit），最大接收单元：物理端口可以接收的最大数据包长度。

PAP（Password Authentication Protocol），口令验证协议：PPP 协议中对通信双方身份认证的安全性协议之一，是一种简单的明文验证协议。PAP 认证仅在 PPP 连接建立时进行。

CHAP（Challenge Handshake Authentication Protocol），质询握手验证协议：PPP 协议中对通信双方身份认证的安全性协议之一，是一种加密的验证方式，能够避免建立连接时传送用户的真实密码。CHAP 认证可以在整个通信过程中进行。

MS-CHAP（Microsoft- Challenge Handshake Authentication Protocol），微软质询握手验证

协议：PPP 协议中对通信双方身份认证的安全性协议之一，与 CHAP 类似，它也是一种加密的验证方式，能够避免建立连接时传送用户的真实密码。MS-CHAP 使用基于 MPPE（微软点对点加密协议）的数据加密。

Fragment，分段：是指在源主机或路由器处，将一个数据包分割成多个数据包的一种过程。经过分段后，每个包都单独传送，并在目的地（目标主机）处重组。

Reassemble，重组：在数据目的地（目标主机）把所有分段重新组合起来的过程。

Peer，对端设备：在 L2TP 协议中，对端设备指 LAC 或 LNS 中的任意一个。LAC 的对端设备是 LNS，反之亦然。

Tunnel，隧道：L2TP 隧道（Tunnel）建立在 LAC 和 LNS 之间，由一个控制连接和 n 个（n ≥0）个会话（Session）组成。控制消息和 PPP 数据包都在隧道上传输。

Session，会话：会话是建立于 LAC 和 LNS 之间的逻辑连接，它必须在隧道建立成功之后（包括身份保护、L2TP 版本、帧类型、硬件传输类型等信息的交换）进行。每个会话连接对应于 LAC 和 LNS 之间的一个 PPP 数据流。

虚端口：用户配置完一条 L2TP 隧道的相关参数后，系统自动生成一个虚端口用来传输数据，该虚端口只能由该用户使用，其他用户不能使用。

监听：虚端口的一种工作状态，在该状态下，LAC 和 LNS 之间并未建立真正的隧道，虚端口一直监听是否有用户的数据包需要传送。

UP：隧道处于连接状态时，路由状态为 UP 状态，表示该路由正在被使用。

DOWN：隧道处于未连接状态时，路由状态为 DOWN 状态，表示该路由未被使用。

MD5（Message Digest 5），消息摘要版本 5：从任意长度信息和 16 字节密钥生成 128 位散列（也称作数字签名或信息整理）的算法。所生成的散列（如同输入的指印）用于验证内容和来源的真实性和完整性。

AAA（Authentication Authorization Accounting），认证授权和记帐：AAA 提供了一个用来对认证、授权和记帐这三种安全功能进行配置的一致性框架。

RADIUS（Remote Access Dial-In User Service），远程访问拨号用户服务：RADIUS 是一个远程访问协议，它通过 Internet 传送认证、授权和记帐信息到远程用户的主网络中。

2.2 L2TP 实现概述

L2TP 协议的基本功能是在 IP 网络中传送采用 PPP 封装的用户的数据包。L2TP 客户端（L2TP Access Concentrator（LAC））负责接收用户的原始数据并封装用户的原始数据包到 PPP 数据包，然后 LAC 与 LNS 建立 L2TP 隧道传送该 PPP 数据包。

如图 2-1 所示，典型的应用通常是 LAC 部署在远程分支机构或移动办公用户的个人电脑软件中，他们用来发起 L2TP 隧道；L2TP 服务器（L2TP Network Server（LNS））部署在企业中心或办公室，用来接收来自 L2TP 客户端 LAC 的呼叫，当 LNS 与 LAC 建立隧道后，LNS 接收来自 LAC 的 PPP 数据包，并还原出用户的数据包，然后把还原后的数据包发送到最终用户的电脑设备上。

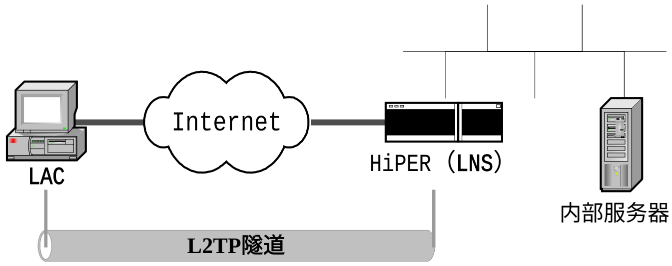


图 2-1 HiPER L2TP 典型应用

HiPER 可以工作 LAC 或 LNS 模式下；或者同时作为 LNS 和 LAC 工作，在这种情况下，LNS 一方面接收来自 LAC 的数据包，另一方面将接收到的数据包发送到其他 LNS 设备中。如图 2-2 所示，对于移动用户来说，HiPER 作为 LNS 接收移动用户的数据，同时 HiPER 又作为 LAC 与公司总部 LNS 相连，从而实现整个企业内部网络的互连。

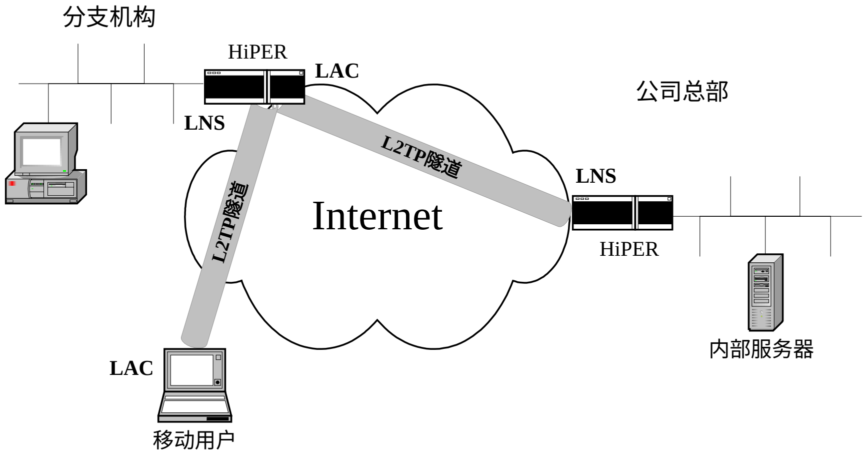


图 2-2 HiPER L2TP 移动用户解决方案

2.2.1 协议

HiPER 中的 L2TP 协议使用 UDP 数据端口 1701 来传输用户数据和隧道控制消息（如隧道建立、维护及终止等），为了使 HiPER L2TP 隧道正常工作，需要以下基本条件：

1. L2TP 客户端和 L2TP 服务器必须有 IP 连接，也就是常说的 IP 路由可达。
2. IP 网络中的防火墙设备必须配置为允许 UDP 1701 端口的数据包通过。

2.2.2 数据流

HiPER 中 L2TP 隧道是通过生成“虚端口”实现的。用户一旦正确的配置了一条 L2TP 的隧道的相关参数，HiPER 系统会使用该配置自动生成一个“虚端口”用来传输数据，该“虚端口”只能由该用户使用，其他用户不能使用。

新生成的端口缺省工作在“监听”（ptpdial）状态下，在该状态下，LAC 和 LNS 之间并未真正建立隧道，以节省系统资源。“监听”状态下的端口一直监听是否有用户的数据包需要传送。

CLI 方式中，可使用 ***show ip route table*** *命令来查看 ptpdial 端口是否建立，处于监听状态。如表 2-1 所示，与该隧道对应路由条目的“IfId”（虚端口标识）处显示为“ptpdial0”，表示 ptpdial 端口已经建立。*

*WEBUI 方式中，可在路由表信息列表（可在**系统状态—>路由和端口信息**中查看）来查看 ptpdial 端口是否建立。如表 2-2 所示，与该隧道对应路由条目的“端口号”处显示为“ptpdial0”，表示 ptpdial 端口已建立。*

IpAddr/Mask	GwIpAddr	IfId	Flag	Cost	Met	Use	Age
192.168.2.0/24	192.168.2.1	ptpdial0	luga	120	7	0	161
192.168.2.1/32	192.168.2.1	ptpdial0	luha	120	7	1	161

表 2-1 CLI 中路由表（部分）

目的地址	网关地址	接口号	路由状态	优先级	跳数	使用次数	使用时间
192.168.18.1/32	-	local	cuhp	20	0	0	86505
192.168.2.0/24	192.168.2.1	ptpdial0	luga	120	7	0	885
192.168.2.1/32	192.168.2.1	ptpdial0	luha	120	7	1	885

表 2-2 WEBUI 中路由表（部分）

当收到第一个用户数据包的时候，LAC 会向 LNS 发出建立隧道传送的请求，LAC 和 LNS 为用户建立隧道的过程中，会经历两次认证过程：

1. 首先，LNS 要确认 LAC 是否是一个合法的发起人，这一阶段叫做“隧道认证”。

CLI 方式中，可使用 ***show session history*** *命令来查看隧道认证是否通过。如图 2-3 所示，在历史信息中有“L2tp UP”相关信息显示，表示隧道认证通过。*

*WEBUI 方式中，可在系统历史记录（可在**系统状态—>系统信息**中查看）来查看隧道认证是否通过。如图 2-4 所示，在系统历史记录中有“L2tp UP”相关信息显示，表示隧道认证通过。*

```
16:54:55          L2tp Up 135.252.52.240
```

图 2-3 CLI 中隧道认证通过信息

```
16:54:55 L2tp Up 135.252.52.240
```

图 2-4 WEBUI 中隧道认证通过信息

2. 其次，通过隧道认证之后再对需要建立隧道的用户进行身份认证，通常叫做“用户认证”。

两次认证通过后，LNS 将接收该呼叫，此时 LAC 和 LNS 间就建立了一条 L2TP 隧道。用户数据就由 LAC 通过该隧道发送到 LNS 上，然后 LNS 把数据发送到接收者所在的网络上，虚端口的状态由“监听”（ptpdial）状态变为“传输”（ptp）状态，与该端口对应的路由也由“DOWN”状态变为“UP”状态。

CLI 方式中，可使用 ***show ip route table*** *命令来查看虚端口是否已由“监听”状态变为“传输”状态。如表 2-3 所示，与该隧道对应路由条目的“IfId”（虚端口标识）处显示为“ptp87”（87 为虚端口号），表示 l2tp 端口已建立，即虚端口已由“监听”状态变为“传输”状态。*

*WEBUI 方式中，可在路由表信息列表（可在**系统状态—>路由和端口信息**中查看）来查看虚端口是否已由“监听”状态变为“传输”状态。如表 2-4 所示，与该隧道对应路由条目的“端口号”处显示为“ptp87”（87 为虚端口号），表示 ptp 端口已建立，即虚端口已由“监听”状态变为“传输”状态。*

```
IpAddr/Mask          GwIpAddr       IfId      Flag       Cost  Met   Use      Age

192.168.2.0/24       10.10.10.11    ptp87     lug         60    1     0        792
192.168.2.1/32       10.10.10.11    ptp87     lugh        60    1     0        792
```

表 2-3 CLI 中路由表（部分）

目的地址	网关地址	接口号	路由状态	优先级	跳数	使用次数	使用时间
192.168.2.0/24	10.10.10.11	ptp87	lug	60	1	0	1348
192.168.2.1/32	10.10.10.11	ptp87	lugh	60	1	0	1348

表 2-4 WEBUI 中路由表（部分）

CLI 方式中，可使用 ***show session userInfo*** *来查看 L2TP 用户信息。如图 2-5 所示，srv 显示为“L2TP ”，表示用户正在使用 L2TP 协议连接。显示信息 “Totoal Active users：1 ”，表示当前有一个 L2TP 用户。需要注意的是此命令可以查看 PPPoE, PPTP, L2TP 等用户的信息，“Totoal Active users ”显示的是总用户数量。*

WEBUI 方式中，无此功能。

```
dir prof/user        callid    port  chan  tx     rx     srv     address
0   vpn/vpn              92     0:-   2:2  n/a    n/a    L2TP    10.10.10.11

Total Active users:          1 , high           1
```

图 2-5 CLI 中 L2TP 用户信息

WEB UI 方式中，可在 “VPN 信息列表 ”（在 ***VPN 配置—>PPTP 和 L2TP*** *中）里面查看 L2TP 用户信息。如表 2-5 所示，“ 状态 ”显示为 “ 已连接 ”，表示 L2TP 隧道已连接。具体描述信息详见章节 5.1.3。*

PPTP/L2TP 信息列表 1/129

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

	设置名	用户名	允许	会话状态	远端网关	远端内网地址	使用时间	
☐	vpn	vpn	☑	已连接	135.252.52.240	192.168.2.1	00:00:37:45	(

表 2-5 WEB UI 中 L2TP 用户信息

如果 LNS 验证 LAC 失败或用户认证失败，LNS 将拒绝该呼叫，由于没有合适的隧道传送该数据包，用户的数据最终被 LAC 丢弃。

CLI 方式中，可使用 ***show ip route table*** *命令来查看虚端口状态。如表 2-6 所示，与该隧道对应路由条目的 “IfId ”（虚端口标识）处显示为 “ptpdial0 ”，表示虚端口仍处在 “ptpdial ”状态，验证失败。*

WEBUI 方式中，可在路由表信息列表（在 ***系统状态—>路由和端口信息*** *中）里面查看虚端口状态。如表 2-7 所示，与该隧道对应路由条目的 “ 端口号 ”处显示为 “ptpdial0 ”，表示虚端口仍处在 “ptpdial ”状态，验证失败。*

```
IpAddr/Mask          GwIpAddr       IfId      Flag       Cost  Met   Use      Age

192.168.2.0/24       192.168.2.1    ptpdial0  luga        120   7     0        161
192.168.2.1/32       192.168.2.1    ptpdial0  luha        120   7     1        161
```

表 2-6 CLI 中路由表（部分）

目的地址	网关地址	接口号	路由状态	优先级	跳数	使用次数	使用时间
192.168.18.1/32	-	local	cuhp	20	0	0	86505
192.168.2.0/24	192.168.2.1	ptpdial0	luga	120	7	0	885
192.168.2.1/32	192.168.2.1	ptpdial0	luha	120	7	1	885

表 2-7 WEBUI 中路由表（部分）

由于在系统中维持一条隧道需要消耗一定的资源，HiPER 采取了一些优化设计。HiPER LAC/LNS 可以被配置成：当没有用户数据需要传送的时候，也就是说该隧道“空闲”（此时虚端口也为“空闲”状态）一段时间后，它将主动拆除已经处在“传输”状态的 L2TP 隧道，虚端口就由“空闲”状态变为“监听”状态，同时相关的路由也变成“DOWN”状态，处在该状态下的隧道不能发送用户数据。

CLI 方式中,通过使用命令 ***set connection/xxx dial idleTimeout xxx*** *来修改"空闲时间"（即 idleTimeout），从而控制隧道空闲后虚端口保持"传输"状态的时间（由"传输"状态变为"监听"状态之前）。*

WEBUI 方式中，通过修改界面参数"空闲时间"（可在 ***VPN 配置—>PPTP 和 L2TP*** *中修改），来控制隧道空闲后虚端口保持"传输"状态的时间（由"传输"状态变为"监听"状态之前）。*

由上，从开始配置 L2TP 隧道参数、到隧道建立、再到隧道断开的整个过程中，相应的虚端口的状态的变化如图 2-6 所示。

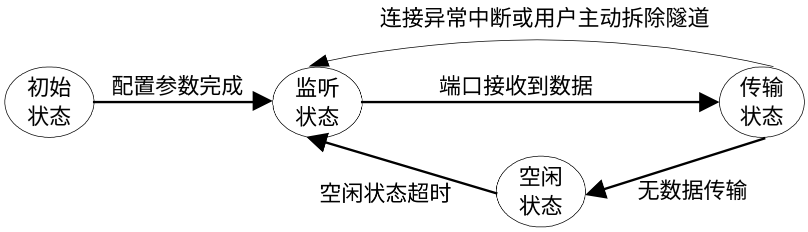


图 2-6 HiPER L2TP 中虚端口状态

提示：虽然 LNS 中也配置了虚端口，但是该端口只能工作在“监听”状态下。即使有数据需要向 LAC 发送，LNS 也不会主动发起建立隧道的请求，这是由于 LAC 的 IP 地址通常都是变化的，因此 LNS 无法确定 LAC 的地址，也就无法发起呼叫请求建立隧道。

2.2.2.1 L2TP 客户端（LAC）数据流

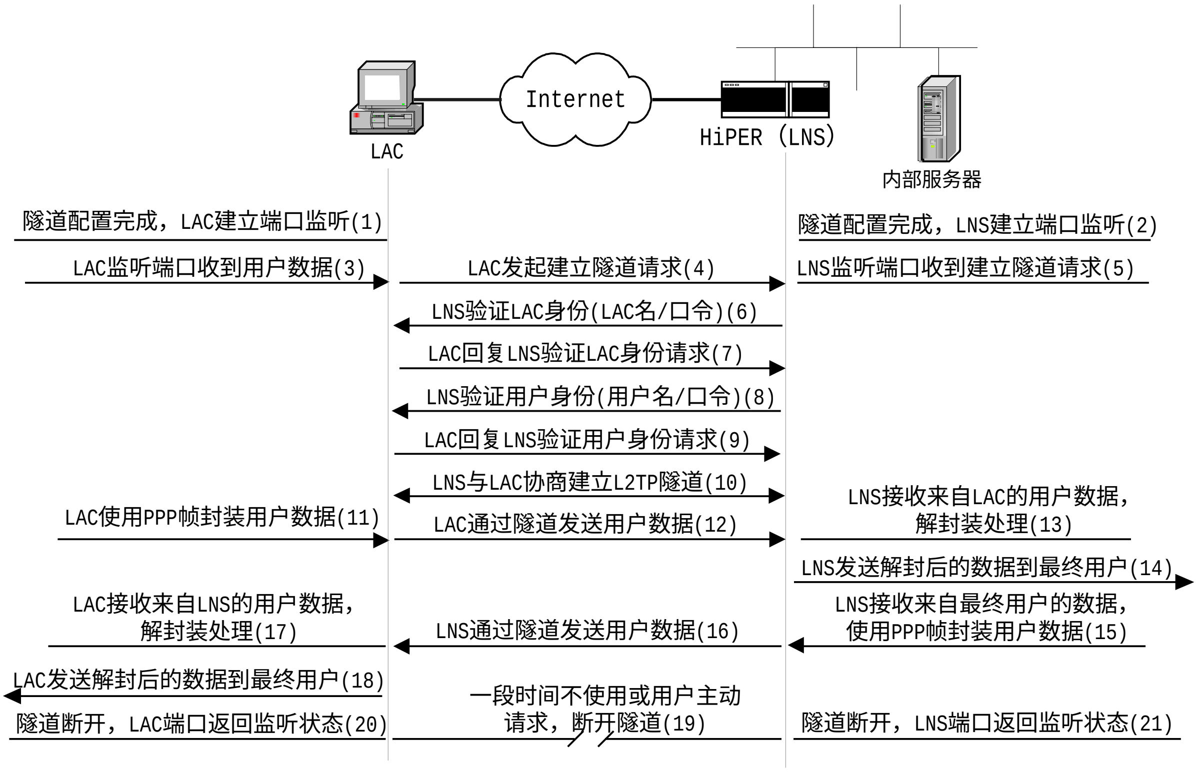


图 2-7 HiPER L2TP 隧道数据流

如图 2-7 所示，L2TP 隧道建立及数据传输的整个过程中，L2TP 客户端（LAC）将依次通过以下数据流：

- 隧道配置完成，LAC 建立虚端口监听（图中（1））；
- LAC 监听端口收到用户数据（图中（3））；
- LAC 发起建立隧道请求（图中（4））；
- LAC 收到 LNS 验证 LAC 身份（LAC 名/口令）请求，回复此请求（图中（7））；
- LAC 收到 LNS 验证用户身份（用户名/口令）请求，回复此请求（图中（9））；
- LNS 与 LAC 协商建立 L2TP 隧道（图中（10））；
- LAC 使用 PPP 帧封装用户数据（图中（11））；
- LAC 通过隧道发送用户数据（PPP 封装）（图中（12））；
- LAC 接收来自 LNS 通过隧道传输的数据，解封装处理（图中（17））；
- LAC 发送解封后的数据到最终用户（图中（18））；
- 隧道空闲一段时间或用户主动请求断开隧道，关闭已建立隧道（图中（19））；
- 隧道断开，LAC 返回监听状态（图中（20））。

2.2.2.2 L2TP 服务器（LNS）数据流

如图 2-7 所示，L2TP 隧道建立及数据传输的整个过程中，L2TP 服务器（LNS）将依次通过以下数据流：

- 隧道配置完成，LNS 建立虚端口监听（此端口只能响应用户的呼叫请求，不能发起呼叫请求）（图中（2））；
- LNS 监听端口收到 LAC 建立隧道请求（图中（5）；

- LNS 要求验证 LAC 身份（LAC 名/口令）（图中（6））；
- LNS 要求验证用户身份（用户名/口令）（图中（8））；
- LNS 与 LAC 协商建立 L2TP 隧道（图中（10）；
- LNS 接收来自 LAC 通过隧道传输的数据，解封装处理（图中（13））；
- LNS 发送解封后的数据到最终用户（图中（14））；
- LNS 接收来自最终用户的数据，使用 PPP 帧封装用户数据（图中（15））；
- LNS 通过隧道发送用户数据（PPP 帧封装）（图中（16））；
- 隧道空闲一段时间或用户主动请求断开隧道，关闭已建立隧道（图中（19））；
- 隧道断开，LNS 返回监听状态（图中（21））。

2.2.3 隧道认证

L2TP 中 LAC 和 LNS 之间建立隧道的过程中可以选择进行隧道认证，这时只有隧道认证通过后才会对拨号用户进行认证。隧道认证通过在 LAC 和 LNS 之间配置“设备 ID/共享密钥”来实现。在“隧道认证”过程中，通过 MD5 消息摘要算法来保证数据传输和认证过程本身的安全。

HiPER 中 L2TP 的实现缺省是不进行 L2TP 隧道认证，这也是绝大部分设备的出厂设置。采用这种配置，可以提高系统的 VPN 处理能力，加快系统建立 VPN 隧道的速度。

CLI 方式中，可以使用命令 ***set ip vpn L2tpAuth enabled*** *改变缺省设置，使得 L2TP 实现需要进行 L2TP 隧道认证。*

WEBUI 方式中，无此功能。

HiPER 在 VPN“拨出”用户中使用“unitname”（主机名）作为 LAC 身份标识，如果“unitname”没有设置，将使用 HiPER 的 MBID 来作为 LAC 身份标识；同时增加密码设置。

CLI 方式中，可以使用命令 ***set system unitname xxx*** *来设置主机名；可以使用命令* ***set conncetion/xxx tunnel secret xxx*** *来设置密码。*

WEBUI 方式中，无此功能。

HiPER 作为 LNS 验证 LAC 用户时候，使用 user 表中的用户名/口令来验证 LAC 是否为合法的 LAC。

CLI 方式中，可以使用命令 ***new user/xxx*** *来设置用户名；可以使用命令* ***set user/xxx passwd xxx*** *来设置用户口令；*

WEBUI 方式中，无此功能。

对于支持 AAA 功能的产品，如果本地没有配置用户，HiPER LNS 将会向 AAA 服务器（通常是 RADIUS 服务器）验证 LAC 的身份信息（根据产品型号决定）。

2.2.4 用户认证

除了需要隧道认证外，实现 L2TP 还需进行用户认证，在这里采用的是 PPP 协议的验证方式。根据实际需要，用户可以选择 PAP 或 CHAP 方式或 PPP 支持的其他验证方式，值得注意的是，必须为同一对 LNS 和 LAC 配置匹配的用户认证方式。

对于 LAC（“拨出”用户），可以选择 PAP、CHAP 或 MS-CHAP 中的一种作为其用户

认证方式。对于 LNS（“拨入”用户），可以选择 PAP、CHAP 或 MS-CHAP 中的一种作为其用户认证方式，LNS 缺省配置可以接受上述的任何一种验证方式。

CLI 方式中，可以使用命令 ***set connection/xxx encaps send authtype pap/chap/mschap*** *设置 LAC 或 LNS 的用户认证方式为 PAP、CHAP 或 MS-CHAP 中的一种。*

WEBUI 方式中，可以选择“密码验证方式”为“PAP”、“CHAP”或“MS-CHAP” 设置 LAC 或 LNS 的用户认证方式为 PAP、CHAP 或 MS-CHAP 中的一种（在 ***VPN 配置—>PPTP 和 L2TP*** *中设置）。*

2.2.5 数据保密

L2TP 协议在传输过程中并不提供数据加密的功能。L2TP 协议是利用 PPP 协议具有的数据压缩/加密功能（如 CCP，PPE 等方式）或利用 IPSec 的加密功能来保护 L2TP 数据的（参考章节 6.4.2、6.4.3）。

2.2.6 MTU 与分段数据传输

L2TP 协议在工作过程中使用了数据封装技术，当用户数据包本身比较大的时候（如 ERP 软件和 FTP 通常会使用比较大的数据包传输数据，MSN/QQ 等聊天软件发送的数据包比较小），封装后的数据可能会超过发送物理端口最大发送单元 MTU（例如以太网接口的最大发送单元 MTU 是 1500 字节，超过 1500 字节大小的数据包将被强制分成多个数据包发送，以确保每个数据包可以被物理端口正确发送），此时数据只能分段传输。在接收方，收到分段后的数据必须组装还原为原来的数据包以后才能进行下一步协议处理，在接收到最后一个分段之前该数据包一直处在待处理状态。如果中间有一个分段丢弃，则整个数据包都被丢弃。

数据分段传输会严重影响系统的性能，所以传输过程中的再分段传输应当尽量避免。为解决此问题，L2TP 协议在隧道建立过程中通过协商 PPP 协议的 MRU/MTU 参数来避免在随后的隧道传输过程中发生数据再分段的情况。

在 HiPER 中可以设置 L2TP 隧道的缺省 MTU（即 tunnelmtu，缺省值为 1400）来调整发送包的大小，超过该 MTU 大小的数据包会主动先分段，然后再发送。同时 HiPER 通过设置每条隧道的 MTU/MRU（用户 MTU/MRU）参数来协商该隧道的 MTU/MRU。正确的配置是 tunnelmtu <用户 MTU≤用户 MRU <最终物理端口的 MTU。

CLI 方式中，可以使用命令 ***set ip vpn tunnelmtu xxx*** *设置隧道的缺省 MTU。*

WEBUI 方式中，无此功能。

CLI 方式中，可以使用命令 ***set connection/xxx encaps mtu xxx*** *设置用户的 MTU；可以使用命令* ***set connection/xxx encaps mru xxx*** *设置用户的 MRU。*

WEBUI 方式中，可以通过设置参数“最大接收单元”的值来设置用户的 MRU（在 ***VPN 配置—>PPTP 和 L2TP*** *中设置），不能设置用户的 MTU。*

下面给出 L2TP 隧道的 MTU（tunnelmtu）的计算实例：

如图 2-8 和如图 2-9 所示，为固定接入和 PPPoE 拨号时，在 L2TP 隧道中传输的封装数据包格式，其中以太网 MTU 及各封装包头大小分别为：

以太网 MTU： 1500 字节；
IP 包头： 20 字节；
UDP 包头： 8 字节；

L2TP 包头（最大）： 30 字节；
PPPoE 包头： 8 字节。

IP 包头	UDP 包头	L2TP 包头	原始IP数据包

图 2-8 L2TP 隧道数据包格式（固定 IP 接入）

PPPoE 包头	IP 包头	UDP 包头	L2TP 包头	原始IP数据包

图 2-9 L2TP 隧道数据包格式（PPPoE 拨号）

因此，固定 IP 接入时（如图 2-8），最大 tunnelmtu 不能大于 l442=1500-20-8-30，单位为字节；如果中间使用 PPPoE 线路（如图 2-9），还要减去 PPPoE 的包头（8 字节），即不能大于 1434=1442-8，单位为字节。

HiPER 中的 L2TP 隧道 MTU（tunnelmtu）缺省值是 1400，可以满足绝大部分应用的要求，一般无须修改。

2.3 L2TP 会话数量限制

针对不同的产品型号，HiPER 中支持 L2TP VPN 隧道的会话数量是不一样的。L2TP 会话数量根据具体的产品规格说明书确定，超过系统支持能力的会话将拒绝。当 VPN 会话数已达最大值时，如果尝试建立新的会话，系统会显示如下信息：



图 2-10 对话框 — VPN 会话数达到最大

CLI 方式中，可使用命令 show session history 查看相关信息，如图 2-11 所示，有“Max VPN sessions。Cannot set up a new L2TP session。”相关信息显示，无法再建立新的 L2TP 会话。

WEBUI 方式中，可在系统历史记录（系统状态—>系统信息中）来查看相关信息。如图 2-12 所示，在系统历史记录中有“Max VPN sessions。Cannot set up a new L2TP session。”相关信息显示，无法再建立新的 L2TP 会话。

```
17:19:32        Max VPN sessions.Cannot set up a new L2TP session.
17:19:29        Ethernet Up
```

图 2-11 CLI 中无法建立新的 L2TP 会话信息

```
17:19:32 Max VPN sessions.Cannot set up a new L2TP session.
17:19:29 Ethernet Up
```

图 2-12 WEBUI 中无法建立新的 L2TP 会话信息

提示：系统保留一个虚端口为拨入用户使用，实际可配 L2TP 隧道相应减少一条。

2.4 小结

本节中我们介绍了 HiPER L2TP 的实现，包括：
L2TP 协议；
HiPER 中 L2TP 数据流的处理；
HiPER 中的“虚端口”概念；
L2TP 隧道只使用一条 UDP1701 端口传送数据，容易穿过防火墙；
L2TP 有隧道认证和用户认证两个验证阶段，隧道认证是可选的。

2.5 协议标准及参考资料

HiPER L2TP 的实现遵守以下标准：

L2TP 协议最重要的标准是 RFC2661（Layer Two Tunneling Protocol（L2TP），第二层隧道协议）；

另外有关 L2TP 中 PPP 协议部分的标准参考 RFC1661（The Point-to-Point Protocol（PPP），点对点协议）。

第3章　HiPER 中 PPTP 的实现

PPTP 协议是一种虚拟专用网协议（VPN），该协议可以完成 PPP 封装的数据包在以太网上的传送，PPTP 协议工作在客户机/服务器（Client/Server）模式下，通信的双方拨出（发起呼叫）的一方叫客户端（Client），拨入（接收呼叫）的一方叫服务器（Server）。使用 PPTP 协议可以在 IP 网（如宽带网）中提供类似于拨号网络（如电话线）的远程接入服务，扩展企业网的范围，实现 VPN 应用。

本章描述了 PPTP 协议在 HiPER VPN 网关中的实现，包括如下内容：

缩略语与专用名词（章节 3.1）

PPTP 实现概述（章节 3.2）

PPTP 会话数量限制（章节 3.3）

小结（章节 3.4）

协议标准及参考资料（章节 3.5）

3.1　缩略语与专用名词

PPTP（Point-to-Point Tunneling Protocol），点到点隧道协议：PPTP 是一种虚拟专用网络协议，属于第二层的协议。PPTP 将 PPP（Point-to-Point Protocol）帧封装在 IP 数据报中，通过 IP 网络如 Internet 或企业专用 Intranet 等发送。

GRE（Generic Routing Encapsulation），基本路由封装：基本路由封装协议是对某些网络层协议（如 IP 和 IPX）的数据报进行封装，使这些被封装的数据报能够在另一个网络层协议（如 IP）中传输。GRE 协议号是 47。

PPP（Point-to-Point Protocol），点对点协议：PPP 协议是为在两点之间传输数据包的简单链路设计的，这些链路提供全双工的操作。

MTU（Maximum Transmission Unit），最大发送单元：物理端口可以发送的最大数据包长度。

MRU（Maximum Receive Unit），最大接收单元：物理端口可以接收的最大数据包长度。

PAP（Password Authentication Protocol），口令验证协议：PPP 协议中对通信双方身份认证的安全性协议之一，是一种简单的明文验证协议。PAP 认证仅在 PPP 连接建立时进行。

CHAP（Challenge Handshake Authentication Protocol），质询握手验证协议：PPP 协议中对通信双方身份认证的安全性协议之一，是一种加密的验证方式，能够避免建立连接时传送用户的真实密码。CHAP 认证在整个通信过程中进行。

MS-CHAP（Microsoft- Challenge Handshake Authentication Protocol），微软质询握手验证协议：PPP 协议中对通信双方身份认证的安全性协议之一，与 CHAP 类似，它也是一种加密的验证方式，能够避免建立连接时传送用户的真实密码。MS-CHAP 使用基于 MPPE（微软点对点加密协议）的数据加密。

Fragment，分段：是指在源主机或路由器处，将一个 IP 包分割成多个 IP 包的一种过程。经过分段后，每个包都单独传送，并在目的地（目标主机）处重组。

Reassemble，重组：在目的地（目标主机）把所有分段按顺序组合起来的过程。

Peer，对端设备：在 PPTP 协议中，对端设备指 PPTP 服务器或 PPTP 客户端中的任意一个。PPTP 服务器的对端设备是 PPTP 客户端，反之亦然。

Tunnel，隧道：PPTP 隧道（Tunnel）建立在 PPTP 服务器和 PPTP 客户端之间，由一个控制连接和 n 个（n≥0）个会话（Session）组成。同一对 PPTP 服务器和 PPTP 客户端之间只能建立一个 PPTP 隧道。控制消息和 PPP 数据包都在隧道上传输。

Session，会话：会话是建立于 PPTP 服务器和 PPTP 客户端之间的逻辑连接，它必须在隧道建立成功之后（包括身份保护、PPTP 版本、帧类型、硬件传输类型等信息的交换）进行。每个会话连接对应于 PPTP 服务器和 PPTP 客户端之间的一个 PPP 数据流。

NAT（Network Address Translation），网络地址转换：NAT 是用于实现内部网络私有地址到外部网络公共地址的转换。

3.2 PPTP 实现概述

PPTP 协议的基本功能是在 IP 网络中传送采用 PPP 封装的用户数据包。PPTP 客户端负责接收用户的原始数据，并将之封装到 PPP 数据包，然后在 PPTP 客户端和服务器之间建立 PPTP 隧道传送该 PPP 数据包。

典型的应用通常是 PPTP 客户端部署在远程分支机构或移动办公用户的个人电脑软件中，他们用来发起 PPTP 隧道；PPTP 服务器部署在企业中心或办公室，用来接收来自 PPTP 客户端的呼叫，当建立起 PPTP 隧道连接后，PPTP 服务器接收来自 PPTP 客户端的 PPP 数据包，并还原出用户的数据包，然后把还原后的数据包发送到最终用户的电脑设备上。

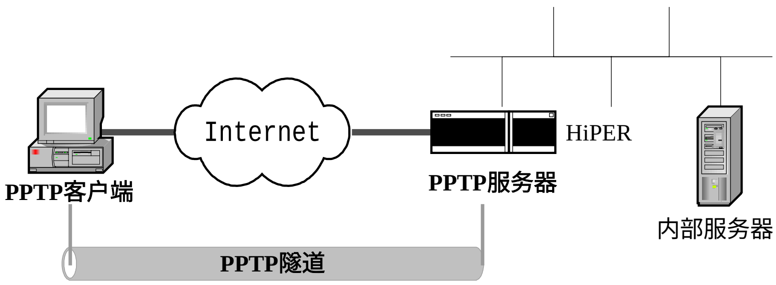


图 3-1 HiPER PPTP 典型应用

HiPER 可以工作 PPTP 客户端或服务器两种模式下；或者同时作为 PPTP 客户端和服务器工作，在这种情况下，PPTP 服务器一方面接收来自 PPTP 客户端的数据包，另一方面将接收到的数据包发送到其他服务器设备中。如图 3-2 所示，对于移动用户来说，HiPER 作为 PPTP 服务器接收移动用户的数据,同时 HiPER 又作为客户端与公司总部 PPTP 服务器相连，实现整个企业网络的互连。

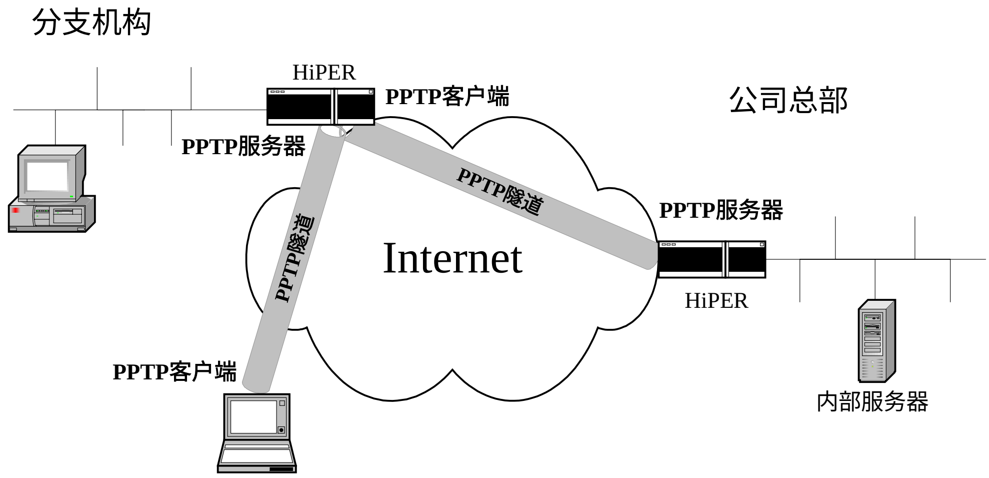


图 3-2 HiPER PPTP 移动用户解决方案

3.2.1 协议

PPTP 通信由以下两部分组成：

1. PPTP 控制连接

一种用以代表 PPTP 隧道并且必须通过一系列 PPTP 消息来创建、维护与终止的逻辑连接。PPTP 控制连接通信过程使用 PPTP 客户端上动态分配的 TCP 端口以及 PPTP 服务器上的 TCP 1723 端口。

2. 针对数据的 GRE 封装

当通过 PPTP 连接发送数据时，PPP 帧将利用通用路由封装（GRE）包头进行封装，这种包头包含了用以对数据包所使用的特定 PPTP 隧道进行标识的信息。原始 GRE 包头则在 RFC 1701 中进行了定义。

PPTP 采用单独的 GRE 数据封装机制对网络地址转换设备（NAT）产生一种有趣的副作用。大多数 NAT 设备能够对基于 TCP 的 PPTP 控制连接内容进行正确的 NAT 转换。然而，很多 NAT 设备和防火墙设备不支持 GRE NAT 转换和传输，具有 GRE 包头的 PPTP 数据包有些情况下将无法通过防火墙或 NAT 设备。HiPER 能够支持 PPTP 隧道穿越防火墙或 NAT 设备。

为了使 PPTP 隧道正常工作，需要以下基本条件：

1. PPTP 客户端和 PPTP 服务端必须有 IP 连接，也就是常说的 IP 路由可达。
2. IP 网络中的防火墙设备必须配置为允许 TCP 1723 端口的数据包通过
3. IP 网络中的防火墙设备必须配置为允许 GRE 类型的数据包通过。

3.2.2 数据流

HiPER 中 PPTP 隧道是通过生成“虚端口”实现的。用户一旦正确配置了一条 PPTP 隧道的相关参数，HiPER 系统会使用该配置自动生成一个“虚端口”用来传输数据，该“虚端口”只能由该用户使用，其他用户不能使用。

新生成的端口缺省工作在“监听”（ptpdial）状态下，在该状态下，PPTP 客户端或服务器并未真正建立“隧道”，以节省系统资源。“监听”状态下的端口一直监听是否有用户的数据包需要传送。

CLI 方式中，可使用命令 ***show ip route table*** *来查看 ptpdial 端口是否建立，处于监听状态。如表 3-1 所示，与该隧道对应路由条目的“IfId”（虚端口标识）处显示为“ptpdial0”，表示 ptpdial 端口已建立。*

*WEBUI 方式中，可在**系统状态—>路由和端口信息**的“路由表信息列表” 中查看 ptpdial 端口是否建立。如表 3-2 所示，与该隧道对应路由条目的“端口号”处显示为“ptpdial0”，表示 ptpdial 端口已建立。*

IpAddr/Mask	GwIpAddr	IfId	Flag	Cost	Met	Use	Age
192.168.2.0/24	192.168.2.1	ptpdial0	luga	120	7	0	161
192.168.2.1/32	192.168.2.1	ptpdial0	luha	120	7	1	161

表 3-1 CLI 中路由表（部分）

目的地址	网关地址	接口号	路由状态	优先级	跳数	使用次数	使用时间
192.168.18.1/32	-	local	cuhp	20	0	0	86505
192.168.2.0/24	192.168.2.1	ptpdial0	luga	120	7	0	885
192.168.2.1/32	192.168.2.1	ptpdial0	luha	120	7	1	885

表 3-2 WEBUI 中路由表（部分）

当收到第一个用户数据包的时候，PPTP 客户端会向服务器发出建立隧道传送的请求，PPTP 服务器收到来自 PPTP 客户端的请求后，会验证该用户是否是一个合法的用户。如果用户是合法的（如用户名/密码匹配），PPTP 服务器将接收该请求，此时 PPTP 客户端和服务器之间就建立了一条 PPTP 隧道，用户数据就由 PPTP 客户端通过该隧道发送到 PPTP 服务器上，然后 PPTP 服务器把数据发送到接收者所在的网络上，虚端口的状态由“监听”（ptpdial）状态变为“传输”（ptp）状态，对应的路由也由“DOWN”状态变为“UP”状态。

CLI 方式中，可使用命令 ***show ip route tabl****e 来查看虚端口是否已由“监听”状态变为“传输”状态。如表 3-3 所示，与该隧道对应路由条目的“IfId”（虚端口标识）处显示为“ptp87”（87 为虚端口号），表示 pptp 端口已建立，即虚端口已由“监听”状态变为“传输”状态。*

*WEBUI 方式中，可在**系统状态—>路由和端口信息**的“路由表信息列表”中查看虚端口是否已由“监听”状态变为“传输”状态。如表 3-4 所示，与该隧道对应路由条目的“端口号”处显示为“ptp87”（87 为虚端口号），表示 ptp 端口已建立，即虚端口已由“监听”状态变为“传输”状态。*

IpAddr/Mask	GwIpAddr	IfId	Flag	Cost	Met	Use	Age
192.168.2.0/24	10.10.10.11	ptp87	lug	60	1	0	792
192.168.2.1/32	10.10.10.11	ptp87	lugh	60	1	0	792

表 3-3 CLI 中路由表（部分）

目的地址	网关地址	接口号	路由状态	优先级	跳数	使用次数	使用时间
192.168.2.0/24	10.10.10.11	ptp87	lug	60	1	0	1348
192.168.2.1/32	10.10.10.11	ptp87	lugh	60	1	0	1348

表 3-4 WEBUI 中路由表（部分）

CLI 方式中，可使用命令 ***show session userInfo*** *来查看 PPTP 用户信息。如图 3-3 所示，srv 显示为“PPTP”，表示用户正在使用 PPTP 协议连接。显示信息“Total Active users：1”，表示当前有一个 PPTP 用户。需要注意的是此命令可以查看 PPPoE、PPTP、L2TP 等用户的信息，“Total Active users”显示的是总用户数量。*

WEBUI 方式中，无此功能。

```
dir prof/user        callid    port  chan  tx     rx     srv     address
I   vpn/vpn              3       0:-  2:2  n/a    n/a    PPTP    10.10.10.11

Total Active users:          1, high         1
```

图 3-3 CLI 中 PPTP 用户信息显示

WEB UI 方式中，可在 ***VPN 配置—>PPTP 和 L2TP*** *的"PPTP/L2TP 信息列表"中查看 PPTP 用户信息。如表 3-5 所示。"状态"显示为"已连接"，表示 PPTP 隧道已连接。具体信息描述详见章节 5.1.3。*

PPTP/L2TP 信息列表 1/6

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

	设置名	用户名	允许	会话状态	远端网关	远端内网地址	使用时间
☐	vpn	vpn	☑	已连接	200.200.200.102	192.168.1.1	00:00:00:18

表 3-5 WEB UI 中 PPTP 用户信息

如果 PPTP 服务器验证 PPTP 用户失败，PPTP 服务器将拒绝该呼叫，由于没有合适的隧道传送该数据报，用户的数据最终被 PPTP 客户端丢弃。

CLI 方式中，可使用命令 ***show ip route table*** *命令来查看虚端口状态。如表 3-6 所示，与该隧道对应路由条目的"IfId"（虚端口标识）处显示为"ptpdial0"，表示虚端口仍处在"ptpdial"状态，验证失败。*

WEBUI 方式中，可在 ***系统状态—>路由和端口信息*** *的"路由表信息列表"中查看虚端口状态。如表 3-7 所示，与该隧道对应路由条目的"端口号"处显示为"ptpdial0"，表示虚端口仍处在"ptpdial"状态，验证失败。*

```
IpAddr/Mask         GwIpAddr        IfId      Flag      Cost  Met  Use     Age

192.168.2.0/24      192.168.2.1     ptpdial0  luga      120   7    0       161
192.168.2.1/32      192.168.2.1     ptpdial0  luha      120   7    1       161
```

表 3-6 CLI 中路由表（部分）

目的地址	网关地址	接口号	路由状态	优先级	跳数	使用次数	使用时间
192.168.18.1/32	-	local	cuhp	20	0	0	86505
192.168.2.0/24	192.168.2.1	ptpdial0	luga	120	7	0	885
192.168.2.1/32	192.168.2.1	ptpdial0	luha	120	7	1	885

表 3-7 WEBUI 中路由表（部分）

由于在系统中维持一条隧道需要消耗一定的资源，HiPER 中采取了一些优化设计。HiPER PPTP 客户端/服务器可以被配置成：当没有用户数据需要传送的时候，也就是说该隧道"空闲"（此时虚端口也为"空闲"状态）一段时间后，它将主动拆除已经处在"传输"状态的 PPTP 隧道，虚端口就由"空闲"状态变为"监听"状态，同时相关的路由也变成"DOWN"状态，处在该状态下的隧道不能发送用户数据。

CLI 方式中，通过使用命令 ***set connection/xxx dial idleTimeout xxx*** *来修改"空闲时间"（即 idleTimeout），从而控制隧道空闲后虚端口保持"传输"状态的时间（由"传输"状态变为"监听"状态之前）。*

WEBUI 方式中，通过修改界面参数"空闲时间"（可在 ***VPN 配置—>PPTP 和 L2TP*** *中修改），来控制隧道空闲后虚端口保持"传输"状态的时间（由"传输"状态变为"监听"状态之前）。*

由上，从开始配置 PPTP 隧道参数、到隧道建立、再到隧道断开的整个过程中，相应的

虚端口的状态的变化如图 3-4 所示。

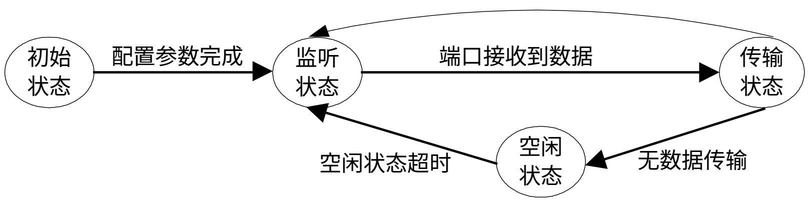


图 3-4 PPTP 中虚端口状态

提示：

虽然 PPTP 服务器也配置了虚端口，但是该端口只能工作在“监听”状态下。即使有数据需要向 PPTP 客户端发送，PPTP 服务器也不会主动发起建立隧道的请求，这是由于 PPTP 客户端的 IP 地址通常都是变化的，因此 PPTP 服务器无法确定 PPTP 客户端的地址，也就无法发起呼叫请求建立隧道。

3.2.2.1 PPTP 客户端数据流

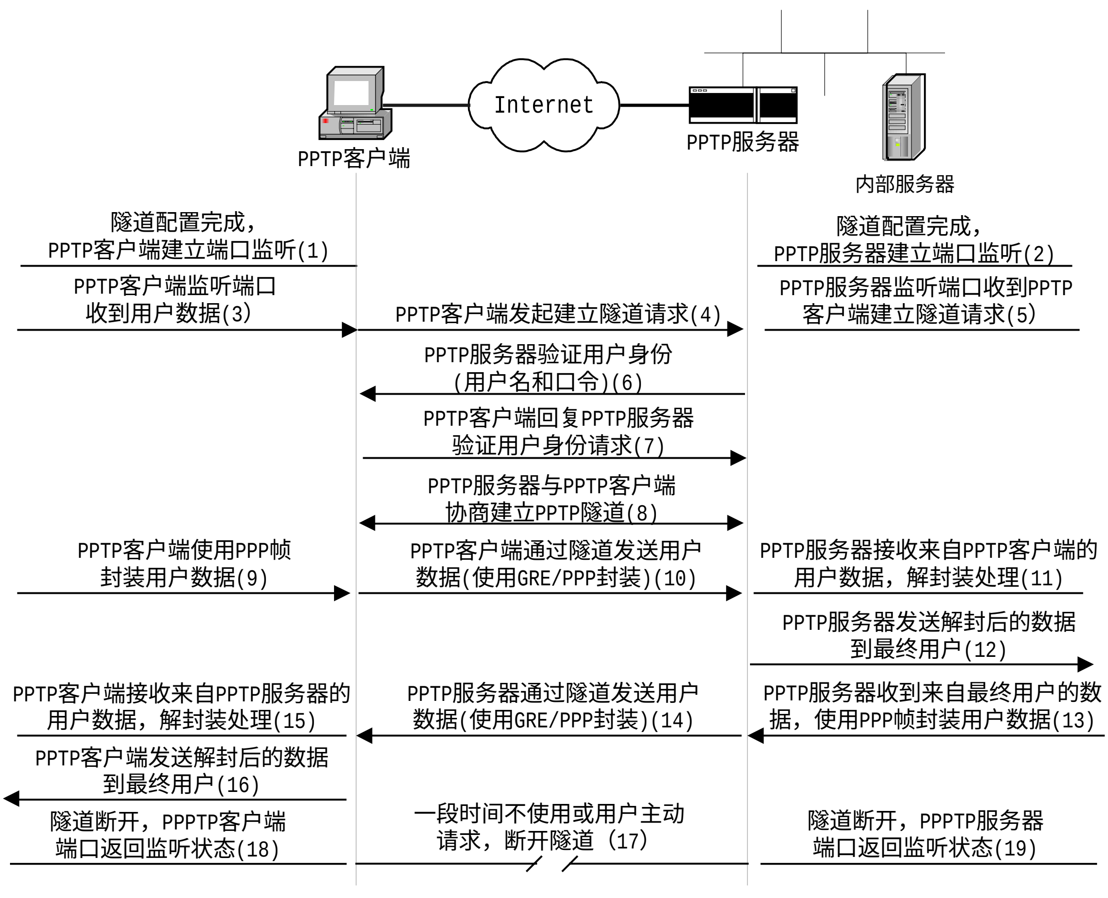


图 3-5 HiPER PPTP 隧道数据流

如图 3-5 所示，PPTP 隧道建立及数据传输的整个过程中，PPTP 客户端将依次通过以下数据流：

- 隧道配置完成，PPTP 客户端建立虚端口监听（图中（1））；
- PPTP 监听端口收到用户数据（图中（3））；

- PPTP 客户端发起建立隧道请求（图中（4））；
- PPTP 客户端收到 PPTP 服务器验证用户身份（用户名/密码）请求，回复此请求（图中（7））；
- PPTP 服务器与 PPTP 客户端建立 PPTP 隧道（图中（8））；
- PPTP 客户端使用 PPP 帧封装用户数据（图中（9））；
- PPTP 客户端通过隧道发送用户数据（GRE/PPP 封装）（图中（10））；
- PPTP 客户端接收来自 PPTP 服务器通过隧道传输的数据，解封装处理（图中（15））；
- PPTP 客户端将发送解封后的数据到最终用户（图中（15））；
- 隧道空闲一段时间或用户主动请求断开隧道，关闭已建立隧道（图中（17）；
- 隧道断开，PPTP 端口返回监听状态（图中（18））。

3.2.2.2 PPTP 服务器数据流

如图 3-5 所示，L2TP 隧道建立及数据传输的整个过程中，PPTP 服务器将依次通过以下数据流：

- 隧道配置完成，PPTP 服务器建立虚端口监听（此端口只能响应用户的呼叫请求，不能发起呼叫请求）（图中（2））；
- PPTP 服务器监听端口收到 PPTP 客户端建立隧道请求（图中（5））；
- PPTP 服务器要求验证用户身份（用户名/口令）（图中（6））；
- PPTP 服务器与 PPTP 客户端协商建立 PPTP 隧道（图中（8）；
- PPTP 服务器接收来自 PPTP 客户端通过隧道传输的数据，解封装处理（图中（11））；
- PPTP 服务器发送解封后的数据到最终用户（图中（12））；
- PPTP 服务器接收来自最终用户的数据，使用 PPP 帧封装用户数据（图中（13））；
- PPTP 服务器通过隧道发送用户数据（GRE/PPP 封装）（图中（14））；
- 隧道空闲一段时间或用户主动请求断开隧道，关闭已建立隧道（图中（17））；
- 隧道断开，PPTP 服务器返回监听状态（图中（19））。

3.2.3 隧道认证

PPTP 协议 PPTP 客户端和服务器建立隧道的过程是不需要验证的。也就是说，PPTP 协议只有用户认证这一个验证过程。

3.2.4 用户认证

在这里采用的是 PPP 协议的验证方式进行用户认证。根据实际需要，用户可以选择 PAP 或 CHAP 方式或 PPP 支持的其他验证方式，值得注意的是，必须为同一对 PPTP 服务器和客户端配置匹配的用户认证方式。

对于 PPTP 客户端（“拨出”用户），可以选择 PAP、CHAP 或 MS-CHAP 中的一种作为其用户认证方式。对于 PPTP 服务器（“拨入”用户），可以选择 PAP、CHAP 或 MS-CHAP 中的一种作为其用户认证方式，PPTP 服务器缺省配置可以接受上述的任何一种验证方式。

CLI 方式中，可以使用命令 ***set connection/xxx encaps send authtype pap/chap/mschap*** *设置 PPTP 客户端或 PPTP 服务器的用户认证方式为 PAP、CHAP 或 MS-CHAP 中的一种。*

WEBUI 方式中，可以选择“密码验证方式”为“NONE”、“PAP”、“CHAP”或“MS-CHAP” 设置 PPTP

客户端或 PPTP 服务器的用户认证方式为 NONE（不验证）、PAP、CHAP 或 MS-CHAP 中的一种（在 ***VPN 配置—>PPTP 和 L2TP*** *中设置）。*

3.2.5 数据保密

PPTP 协议在传输过程中并不提供数据加密的功能，PPTP 协议是利用 PPP 协议具有的数据压缩/加密功能（如 CCP、PPE 等方式）或利用 IPSec 的加密功能来保护 PPTP 数据（参考章节 6.4.2、章节 6.4.3）。

3.2.6 MTU 与分段数据传输

PPTP 协议在工作过程中使用了数据封装技术，当用户数据包本身比较大的时候（如 ERP 软件和 FTP 通常会使用比较大的数据包传输数据，MSN/QQ 等聊天软件发送的数据包比较小），封装后的数据可能会超过发送物理端口最大发送单元 MTU（例如以太网接口的最大发送单元 MTU 是 1500 字节，超过 1500 字节大小的数据包将被强制分成多个数据包发送，以确保每个数据包可以被物理端口正确地发送），此时数据只能分段传输。在接收方，收到分段后的数据必须组装还原为原来的数据包以后才能进行下一步协议处理，在接收到最后一个分段之前该数据包一直处在待处理状态。如果中间有一个分段丢失，则整个数据包将被丢弃。

数据分段传输会严重影响系统的性能，所以传输过程中的再分段传输应当尽量避免。为解决此问题，PPTP 协议在隧道建立过程中通过协商 PPP 协议的 MRU/MTU 参数来避免在随后的隧道传输过程中发生数据再分段的情况。

在 HiPER 中可以设置 PPTP 隧道的缺省 MTU（即 tunnelmtu，缺省值为 1400）来调整发送包的大小，超过该 MTU 大小的数据包会主动先分段，然后再发送。同时 HiPER 通过设置每条隧道的 MTU/MRU（即用户 MTU/MRU）参数来协商该隧道的 MTU/MRU。正确的配置是 tunnelmtu <用户 MTU≤用户 MRU <最终物理端口的 MTU。

CLI 方式中，可以使用命令 ***set ip vpn tunnelmtu xxx*** *设置隧道的 MTU。*

WEBUI 方式中，无此功能。

CLI 方式中，可以使用命令 ***set connection/xxx encaps mtu xxx*** *设置用户的 MTU；可以使用命令* ***set connection/xxx encaps mru xxx*** *设置用户的 MRU。*

WEBUI 方式中，可以通过设置参数“最大接收单元”的值来设置用户的 MRU（在 ***VPN 配置—>PPTP 和 L2TP*** *中设置），不能设置用户的 MTU。*

下面给出 PPTP 隧道的 MTU（tunnelmtu）的计算实例：

如图 3-6 和如图 3-7 所示，为固定 IP 接入和 PPPoE 拨号时，在 PPTP 隧道中传输的封装数据包格式，其中以太网 MTU 及各封装包头大小分别为：

以太网 MTU：　1500 字节；
IP 包头：　20 字节；
GRE 包头：　8 字节；
PPTP 包头（最大）：　30 字节；
PPPoE 包头：　8 字节；

IP 包头	GRE 包头	PPTP 包头	原始IP数据包

图 3-6 PPTP 隧道数据包格式（固定 IP 接入）

PPPoE包头	IP包头	GRE包头	PPTP包头	原始IP数据包

图 3-7 PPTP 数据包格式（PPPoE 拨号）

因此，固定 IP 接入时（如图 3-6），最大 tunnelmtu 不能大于 1442=1500-20-8-30，单位为字节；如果中间使用 PPPoE 线路（如图 3-7），还要减去 PPPoE 的包头（8 字节），不能大于 1434=1442-8，单位为字节。

HiPER 中的 PPTP 隧道 MTU 缺省值是 1400，可以满足绝大部分应用的要求，一般无须修改。

3.3 PPTP 会话数量限制

针对不同的产品型号，HiPER 支持 PPTP VPN 隧道的会话数量是不一样的。PPTP 会话数量根据具体的产品规格说明书确定，超过系统支持能力的会话将被拒绝。当 VPN 会话数已达最大值时，如果尝试建立新的会话，系统会显示如下信息：



图 3-8 对话框 — VPN 会话数达到最大

CLI 方式中，可使用命令 show session history 查看相关信息，如图 3-9 所示，有“Max VPN sessions。Cannot set up a new PPTP session。”相关信息显示，无法再建立新的 PPTP 会话。

WEBUI 方式中，可在系统状态—>系统信息的“系统历史记录”中查看相关信息。如图 3-10 所示，在系统历史记录中有“Max VPN sessions。Cannot set up a new PPTP session。”相关信息显示，无法再建立新的 PPTP 会话。

```
17:19:32        Max VPN sessions.Cannot set up a new PPTP session.
17:19:29        Ethernet Up
```

图 3-9 CLI 中无法建立新的 PPTP 会话信息

```
17:19:32 Max VPN sessions.Cannot set up a new PPTP session.
17:19:29 Ethernet Up
```

图 3-10 WEBUI 中无法建立新的 PPTP 会话信息

提示：系统保留一个虚端口为拨入用户使用，实际可配 PPTP 隧道相应减少一条。

3.4 小结

PPTP与L2TP对比如下：

PPTP 协议也是一种在 IP 网络中传输 PPP 数据包的方法，开发者为 Microsoft 公司，从协议的角度来看，可以说是 L2TP 的前身，L2TP 就是以 PPTP 协议为基础，由 IETF 组织制定的标准 VPN 协议。PPTP 现在已经是 IETF 标准，RFC2637。

1. PPTP 的优点

   在 Windows 平台中支持，包括老版本 Win98，无须另外软件。

2. PPTP 的缺点
   1) 早期的 Microsoft PPTP 实现有比较大的安全漏洞，容易导致黑客攻击；
   2) PPTP VPN 需要两个连接，有时会导致连接状态不一致（TCP 连接正常，但是 GRE 不正常）；
   3) 很多 NAT/防火墙设备不支持 GRE 数据包通过，而 GRE 通不过则会导致 VPN 建立失败。

3.5 协议标准及参考资料

HiPER PPTP 的实现遵守以下标准：

PPTP 协议最重要的标准是：RFC2637（Point-to-Point Tunneling Protocol（PPTP），点对点隧道协议）；

另外有关 PPTP 中 PPP 协议部分的标准参考 RFC1661（The Point-to-Point Protocol（PPP），点对点协议）。

第4章 HiPER 中 IPSec 实现

随着安全标准与网络协议的不断发展，各种 VPN 技术层出不穷，IPSec VPN 则是当前应用最广泛的 VPN 安全技术之一。

IPSec是创建和维持IP网络安全通信的一套开放标准、协议，它提供两种安全机制：加密和认证。加密机制保证了数据的机密性，认证机制保证了数据是来自原始的发送者并且在传输过程中没有被破坏和篡改。

本章描述了 IPSec 协议在 HiPER VPN 网关中的实现，包括如下内容：

缩略语与专用名词（章节 4.1）

IPSec 实现概述（章节 4.2）

IPSec NAT 穿透（章节 4.3）

IPSec 会话数量限制（章节 4.4）

小结（章节 4.5）

协议标准及参考资料（章节 4.6）

4.1 缩略语与专用名词

IPSec（IP Security Protocol），IP 网络安全协议：IPSec 是 IETF 制定的一系列协议，以保证在 Internet 上传送数据的安全保密性，通信双方在 IP 层通过加密与数据源验证来保证数据包在 Internet 上传输时的私有性、完整性和真实性。

DES（Data Encryption Standard），数据加密标准：DES 是 IPSec 使用的一种数据加密算法，用于对数据包进行加密。

3DES（Triple Data Encryption Standard），三倍数据加密标准：3DES 是 IPSec 使用的一种数据加密算法，用于对数据包进行比 DES 强度更高的加密。

AES（Advanced Encryption Standard），高级加密标准：AES 是 IPSec 使用的一种数据加密算法。与 DES 和 3DES 相比，AES 更加高效、安全。

ISAKMP（Internet Security Association and Key Mangement Protocol），因特网安全联盟和密钥管理协议：ISAKMP 提供了验证对方身份的方法、密钥交换时交换信息的方法以及对安全服务进行协商的方法。

IKE（Internet Key Exchange），因特网密钥交换：IKE 用于通信双方协商和建立安全联盟、交换密钥。IKE 定义了通信双方进行身份验证、协商加密算法以及生成共享密钥的方法。

DH（Diffie-Hellman Group），一种密钥交换算法：通信的双方各自生成一对公/私钥，只需和对方交换公钥，经过计算就可得到一组用来保护通信的密钥，这就避免了直接在通信中传输密钥的风险，提高了整个 IPSec 系统的安全性。DH 有一个重要的属性：group（组件），共有 5 种基本 group，常用的 group 有：模数为 768 位的 MODP 组（group1）、模数为 1024 位的 MODP 组（group2）、模数为 1680 位的 MODP 组（group5）。

MD5（Message Digest 5），消息摘要版本 5：从任意长度信息和 16 字节密钥生成 128 位散列（也称作数字签名或信息整理）的算法。所生成的散列（如同输入的指印）用于验证内容和来源的真实性和完整性。

SHA-1（Secure Hash Alogrithm1），安全散列算法 1：从任意长度信息和 20 字节密钥生成 160 位散列的算法。通常认为它比 MD5 更安全，因为它生成的散列更大。

Tunnel Mode，隧道模式：IPSec 有两种运行模式，一种是保护 IP 包中的上层协议数据，另一种是保护整个数据包。其中，隧道模式是用来保护整个数据包的，它要对整个 IP 数据包进行封装和保护。

Transport Mode，传送模式：IPSec 有两种运行模式，一种是保护 IP 包中的上层协议数据，另一种是保护整个数据包。其中，传送模式只保护 IP 包中的上层协议数据，它只对 IP 数据包中的有效负载进行封装和保护。

MTU（Maximum Transmission Unit），最大发送单元：物理端口可以发送的最大数据包长度。

SA（Security Association），安全联盟：在两个设备之间建立一个 IPSec VPN 隧道并通过其进行安全通信之前，它们必须就通信期间需要使用的安全参数达成一致，即建立一个 SA。SA 将指定需要使用的认证与加密算法、在通话期间使用的密钥和安全联盟本身需要维持的时间，SA 是单向的。

SPI（Security Parameter Index），安全参数索引：SPI 实际上是一个长度为 32 位的数据实体，用于独一无二地标识出接收端上的一个 SA。

AH（Authentication Header），认证包头：属于 IPSec 的一种协议。该协议用于为 IP 数据包提供数据完整性、数据包源地址验证和一些有限的抗重播服务。与 ESP 协议相比，AH 不提供对通信数据加密服务，但能比 ESP 提供更加广的数据验证服务。

ESP（Encapsulating Security Payload），封装安全负荷：属于 IPSec 的一种协议。它用于确保 IP 数据包的机密性（对第三方不可见）、数据的完整性以及对数据源地址的验证，同时还具有抗重播的特性。

PSK（Pre-Shared Key），预共享密钥：IKE 身份验证方法之一，它要求每个 IKE 对等方使用一个预定义和共享的密钥来对 IKE 交换执行身份验证。

IPSec 隧道：IPSec 隧道是点对点的安全“连接”。通过在 IPSec 隧道的两端，本端和对端，配置（或自动生成）对应的安全联盟，实现在本端对 IP 数据包加密，在对端解密。IPSec 隧道可以跨越多台路由器和多个网络，只有 IPSec 隧道的两端共享秘密，对于隧道中间的路由器和网络，所有的加密数据包和普通数据包一样被透明地转发。

第一阶段和第二阶段：采用互联网密钥交换协议（IKE）建立 IPSec 通道安全联盟（SA），需要进行两个阶段的协商。在第一阶段，参与者相互验证身份并协商建立一个用来协商随后 IPSec SA 的安全通道。在第二阶段，参与者协商并建立用于加密和认证用户数据的 IPSec SA。

Main Mode and Aggressive Mode，主模式和野蛮模式：IKE 自动协商通道的第一阶段，可以在主模式和野蛮模式这两种模式下进行。主模式下，发起方和响应方之间进行三次双向信息交换，总共六条信息。野蛮模式下，发起方和响应方获取相同的对象，但仅进行两次交换，总共有三条消息。

DPD（Dead Peer Detect）：周期对端检测：使用 DPD，能够定期检测 SA 对方是否正常，网络连接是否正常。

IPSec NAT-T（NAT-Traversal），IPSec NAT 穿透技术：该技术实现了 IPSec 协议穿透 NAT 设备。

4.2 IPSec 实现概述

HiPER IPSec VPN 支持四种 VPN 配置方式：
方式一：“ 手动 ” 方式，网关到网关，使用手动密钥交换；
方式二：“ 自动 ” 方式，网关到网关，使用自动 IKE，主模式；
方式三：“ 自动 ” 方式，动态连接到网关，使用自动 IKE，野蛮模式；
方式四：“ 自动 ” 方式，对方动态连接到本地，使用自动 IKE，野蛮模式。

上述方式一和方式二，均用于 HiPER VPN 网关与远程 VPN 网关的连接，要求通信两端都使用固定 IP 地址。方式三和方式四均使用“ 拨号 ”方式，方式三允许 HiPER VPN 网关使用动态 IP 地址连接到远程网关，方式四允许客户或者远程网关使用动态 IP 地址连接到 HiPER VPN 网关。在后两种方式下，只要一方有固定 IP 地址或者域名。

HiPER 的远程网关支持使用域名代替 IP 地址，HiPER 会自动完成域名到 IP 地址的转换，该功能与 HiPER DDNS 功能配合使用，可以实现在通信双方都没有固定 IP 地址的情况下建立 IPSec VPN。

4.2.1 协议

在两个设备之间建立一个 IPSec VPN 隧道并通过其进行安全通信之前，它们必须就通信期间需要使用的安全参数达成一致，即建立一个安全联盟 SA。SA 是由一对指定的安全参数索引 (SPI) 、目标 IP 地址以及使用的安全协议（认证包头 AH 或封装安全负荷 ESP）组成。

通过 SA，IPSec 隧道可以提供以下安全功能：

- 机密性（通过加密）
- 内容完整性（通过数据认证）
- 发送方认证和认可（通过身份认证）

在实际使用时，根据不同的安全需求, 可以采取不同的安全策略。

如果仅需认证 IP 包来源和内容的完整性，可以不使用任何加密而仅认证此数据包（使用 AH 或者 ESP)。如果仅想保护私密性，可以不使用任何认证机制而对此数据包加密（使用 ESP)。当然，也可以同时加密和认证此数据包（使用 AH+ESP 或 ESP)。大多数网络安全设计者都选择加密、认证及抗重播，这是目前在 IP 网络上能够提供的最高级别的数据保护服务。

IPSec 体系结构如图 4-1 所示。

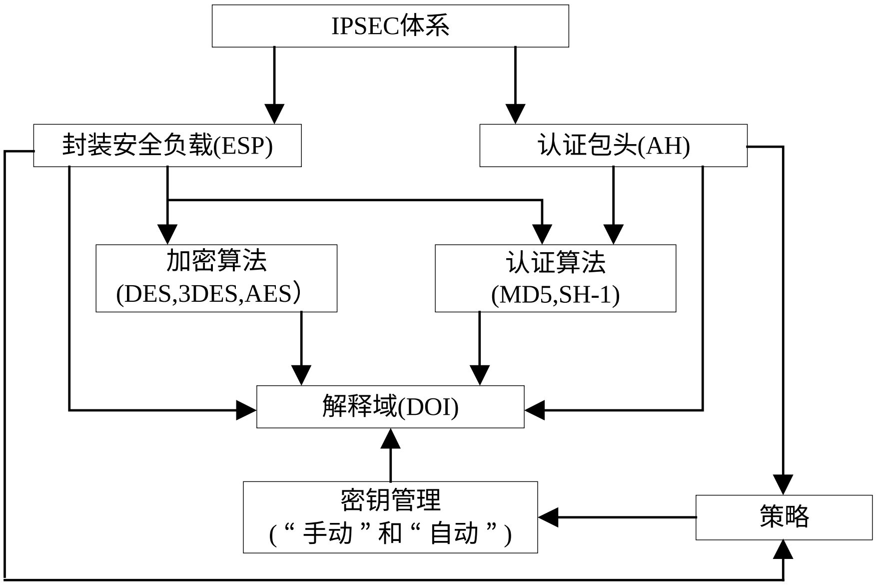


图 4-1 IPSec 体系结构

HiPER 支持 IPSec 技术，使用两种密钥管理/创建机制来创建 VPN 安全联盟（SA）：

· 使用手动密钥交换的“手动”方式
· 使用 IKE 协议（具有预共享密钥）的“自动”方式

4.2.1.1 IPSec 模式

IPSec 有两种运行模式：传送模式（Transport Mode）和通道模式(Tunnel Mode)。传送模式只对原 IP 数据包的有效载荷进行封装和保护，通道模式要对整个 IP 数据包进行封装和保护。

当 IPSec 隧道两端都是主机时，可以使用传送模式或通道模式。当隧道两端至少有一个是安全网关（例如，路由器或防火墙）时，就必须使用通道模式。HiPER 设备总是对 IPSec 运行通道模式。

1. 通道模式

整个原始 IP 数据包（包头和载荷）都封装在另一个 IP 负荷中（如图 4-2 所示），并且附加了新包头，新包头的源地址和目的地址分别是 IPSec 通道的两个端点的 IP 地址。整个原始数据包可以被加密、被认证、或者既加密又认证。如果使用 AH，AH 包头和新包头可被认证。如果使用 ESP，ESP 包头可以被认证。

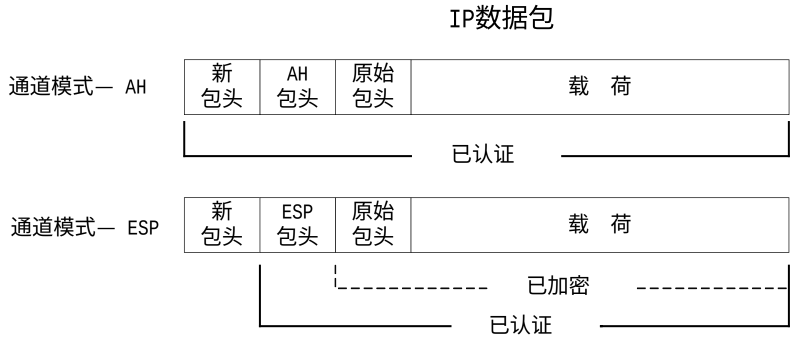


图 4-2 通道模式

2. 传送模式

原始 IP 封包没有封装在另一个 IP 数据包中（如图 4-3 所示）。整个封包都可以认证（使用 AH），负荷可以加密（使用 ESP），原始包头仍保留明文。

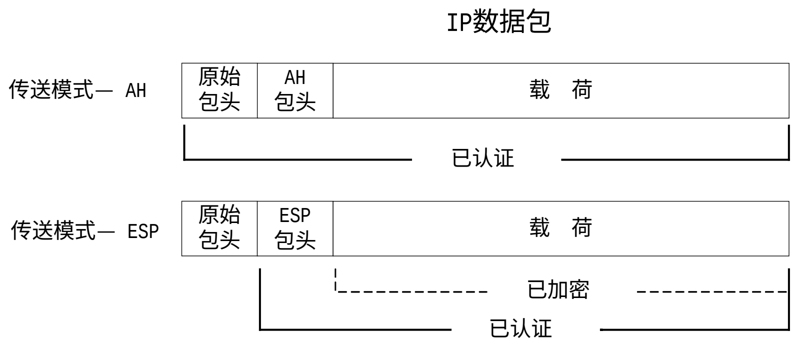


图 4-3 传送模式

4.2.1.2 密钥管理

密钥的分配和管理对于成功创建和使用 IPSec 隧道很关键，它也是实现数据认证和加密的基础。HiPER VPN 网关的 IPSec 配置支持“手动”和“自动”密钥分配方法。

1. “手动”密钥

所谓“手动”密钥，就是在配置 IPSec 隧道时，隧道两端的管理员需要手工配置设备所有的安全参数，通常每个设备有 20 个以上的参数需要配置。

对于小的(例如只有几台设备)的网络来说，这是可行的，在这种网络中，密钥的分配、维护和跟踪都不难。但是，在设备数量较多，设备之间的距离又比较遥远的大型网络中，采用这种配置方式就存在安全问题。因为除了面对面传输密钥外，无法完全保证在传输过程中不泄漏密钥；同时，每当要更改密钥时，像最初分配密钥时一样，需要对所有的设备重新分发新的密码。因此，“手动”方式只适合比较小型的网络使用。

2. “自动”密钥

当需要创建和管理多个 IPSec 隧道时，就需要一种不必为每个设备都配置所有 IPSec 参数的方法。IPSec 使用 IKE 支持密钥的自动生成和协商以及安全联盟的维护，HiPER VPN 网关将之称为“自动”方式，HiPER 使用的是带有预共享密钥的“自动”方式。

预共享密钥是用于生成 IPSec 会话中使用的密钥的“种子密钥”。IPSec 隧道双方在开始通信前都必须拥有此密钥。在“自动”方式下，配置隧道时，密钥的分发与使用“手动”方式时相同。但是，一旦预共享密钥分发完毕后，“自动”方式下的隧道就可使用 IKE 协议，在管理员预先设定的时间间隔内自动更改密钥（与“手动”方式不同），而无须人工参与，降低管理负担。

经常更改密钥会提高安全性，自动更改密钥会减少密钥管理任务。但是，更改密钥会增加流量开销，因此，过于频繁地更改密钥会降低数据传输效率。

4.2.1.3 安全联盟建立

安全联盟（SA）是 IPSec 隧道双方用于确保隧道安全的有关方法和参数的单向协议。对于 IPSec 双向通信，至少必须有两个 SA，一个用来接收来自对端的数据，叫做“进入”；一个用来发送数据给对方，叫做“外出”。

对于通过“手动”密钥方式配置 IPSec 隧道来说，由于已经预先定义了 SA 的所有参数，配置完毕后 SA 就自然建立了。事实上，由于已经建立了该隧道，当接收到的数据包与该隧道配置的策略相匹配时，HiPER VPN 网关将对该数据进行加密和认证，并将其转发到目标网关。

对于通过“自动”密钥方式配置 IPSec 隧道来说，建立 SA，需要进行两个阶段的协商：

- 在第一阶段，通信双方协商如何保护以后的通信，建立一个已通过身份认证和安全保护的通道（即 IKE SA），此通道将用于保护后面的 IPSec SA 的协商过程。
- 在第二阶段，通信双方为 IPSec 协商加密算法、密钥、生存周期以及认证身份，建立用于加密和认证用户数据的通道（即 IPSec SA）。

1. 第一阶段

“自动”密钥通道协商的第一阶段可以使用野蛮模式（Aggressive Mode）或主模式（Main Mode），不管使用哪种模式，双方均将交换对方可以接受的安全提议，例如：

- 加密算法（DES 和 3DES）和认证算法（MD5 和 SHA-1）
- Diffie-Hellman 组（请参阅本节的“Diffie-Hellman 交换”）
- 预共享密钥

当隧道的两端都同意接受所提出的至少一组第一阶段安全参数，并处理相关参数时，一个成功的第一阶段协商将结束。HiPER VPN 网关作为发起方时，最多同时支持 12 个第一阶段协商的提议，允许用户定义一系列安全参数；作为响应方时，可接受任何组合形式的第一阶段协商的提议。

HiPER 提供的预定义的第一阶段提议如下：

- 3des-md5-group2
- 3des-sha-group2
- des-md5-group2
- des-sha-group2

用户也可以自定义第一阶段提议。

*WEB UI 方式下，在 **VPN 配置—>IPSec** 中，可配置“安全选项”中的“预共享密钥”；在 **VPN 配置—>IPSec** 的“高级选项”中，可配置 “加密认证算法 1，2，3，4（第一阶段）”，一次最多配置 4 组提议（章节 6.1.1）。*

➢ **主模式和野蛮模式（Main Mode / Aggressive Mode）**

第一阶段可能发生在野蛮模式或主模式下，这两种模式如下所述：

主模式：发起方和响应方之间进行三个双向信息交换（总共六条信息）以完成以下功能：

- 第一次交换，（信息 1 和 2）：提出并接受加密和认证算法。
- 第二次交换，（信息 3 和 4）：执行 Diffie-Hellman 交换，发起方和响应方各提供一个当前数（随机生成的号码）。
- 第三次交换，（信息 5 和 6）：发送并验证其身份。

在第三次交换信息时传输的信息由在前两次交换中建立的加密算法保护。因此，在明文中没有传输参与者的身份，从而提供了最大限度的保护。

*WEB UI 方式下，在 **VPN 配置—>IPSec** 中，“协商模式”选择为“主模式”即可（章节 6.1.1）。*

野蛮模式：发起方和响应方获取相同的对象，但仅进行两次交换，总共有三条消息：

- 第一条消息：发起方建议 SA，发起 Diffie-Hellman 交换，发送一个当前数及其 IKE 身份。
- 第二条消息：响应方接受 SA，认证发起方，发送一个当前数及其 IKE 身份，以及发送响应方的证书（如果使用证书）。

- 第三条消息：发起方认证响应方，确认交换。

由于参与者的身份是在明文中交换的（在前两条消息中），故野蛮模式不提供身份保护。

WEB UI 方式下，在 ***VPN 配置—>IPSec*** *中，"协商模式"选择为"野蛮模式"即可（章节 6.1.1）。*

提示：当 IP 地址不固定的用户使用"自动"方式（带有预定义密钥）协商 IPSec SA 时，必须使用野蛮模式。

➢ **Diffie-Hellman** 交换

Diffie-Hellman 交换也称"DH 交换"，它允许双方生成一个共享密钥。该技术的优点在于它允许通信双方在非安全媒体上创建密钥，而不必把预共享密钥通过网络传输。共有五种基本 DH 组（HiPER 支持组 1、2 和 5），在各组计算中所使用主要模数的大小都不同，如下所述：

- DH 组 1：768 位模数
- DH 组 2：1024 位模数
- DH 组 5：1536 位模数

模数越大，就认为生成的密钥越安全；但是，模数越大，密钥生成过程就越长。

提示：

由于每个 DH 组的模数大小都不同，因此 IPSec 隧道通信双方必须使用相同的组。

WEB UI 方式下，在 ***VPN 配置—>IPSec*** *的"高级选项"中配置"加密认证算法 1，2，3，4（第一阶段）"时选择 DH 组（章节 6.1.1）。*

2. 第二阶段

当通信双方建立了一个已认证的安全通道后，将继续执行第二阶段，在此阶段中，将协商 IPSec SA 以保护要通过 IPSec 隧道传输的用户数据。

与第一阶段的过程相似，通信双方交换提议以确定要在 SA 中使用的安全参数。第二阶段提议还包括一个安全协议（封装安全负荷（ESP）或认证包头（AH））和所选的加密和认证算法。如果需要完全前向保密（PFS），提议中还可以指定一个 Diffie-Hellman 组。HiPER 目前暂不支持 PFS。

不管在第一阶段中使用何种模式，第二阶段总是在"快速"模式中运行，并且包括三条消息的交换。

WEB UI 方式下，在 ***VPN 配置—>IPSec*** *中，可配置"安全选项"中的"加密认证算法 1"。在* ***VPN 配置—>IPSec*** *的"高级选项"中，可配置"加密认证算法 2，3，4（第二阶段）"，一次最多可配置 4 组第二阶段提议（章节 6.1.1）。*

4.2.1.4 安全联盟维护

一旦 SA 建立完毕，IPSec 双方还必须维护 SA，确保 SA 是安全有效的，IPSec 通过以下方法实现 SA 的有效性检测：

1. SA 生存时间

在建立 SA 的协商过程中，双方会协商该 SA 的生存时间和最大流量，当生存时间或最大流量到达预先设定的值时，需要重新协商以建立新的 SA。周期性的重新协商，相当于定期更改密码。

WEB UI 方式下，在 ***VPN 配置—>IPSec*** *的"高级选项"中，可配置"生存时间"和"最大流量"（章节 6.1.1）。*

由于频繁重建 SA 需要消耗大量的系统资源（主要是 DH 交换和当前数生成），会降低

数据传输效率。因此 SA 的生存时间通常设置的比较长（典型的是 1 小时到 1 天），在有效期内，由于双方不能互相检测对方（类似 PING 的功能），通信的双方只能“假设”对方是正常工作的，万一有一方发生了不可预见的问题或连接双方的网络有故障，通信的另一方并不知道此时双方的连接线路中断，还会继续向早已经不存在的另一方发送数据，造成虚假连接（SA 正常，发出正常，但无法完成双向通信），因此需要一种有效的方法来检测参与 IPSec SA 的双方都完全正常，他们之间的网络连接也完全正常。这种检测方法的开销要比重新协商 IPSec SA 更小，因此可以用更高的密度进行检测。这种技术就是 IPSec“DPD”，DPD 作为 SA 协商的一种补充而存在。

2. DPD（Dead Peer Detect）

只有使用“自动”密钥协商的 IPSec SA 才拥有此功能。IPSec DPD 定期检测 SA 对方是否还存在，在 SA 的生存时间和最大流量范围内，定期检测对方网络是否可达，程序是否正常，以便发现网络变化导致的通信故障或避免与一个已经不存在的“火星人”主机保持 SA，这个检测周期通常为 20 秒或 1 分钟左右，双方通过发送“心跳”包来检测对方是否正常，连续丢失多个心跳包后，IPSec DPD 会强制重新发起 SA 协商。

*WEB UI 方式下，在 **VPN 配置—>IPSec** 的“高级选项”中，可通过选中“DPD”选项来启用 DPD 功能，可通过配置“心跳”来确定检测周期（章节 6.1.1）。*

4.2.2 数据流.

IPSec 协议工作在对等模式下，需要的一方可以随时发起 IPSec 协商。然而，在实现中为了区分隧道的方向，通常把最先发起 IPSec 协商的一端叫“发起方/客户端”，把响应该发起请求的一方叫做“响应方/服务端”。

“野蛮模式”下的 IPSec 隧道，因为移动用户的 IP 地址不能确定，拥有固定 IP 地址的一方无法主动发起 IPSec 隧道，在这种模式下，IPSec 隧道只能由移动用户发起，也就是说，移动用户永远是“发起方”。

HiPER 中 IPSec 隧道是通过生成“安全虚端口”实现的，该端口与 PPTP/L2TP VPN 使用的“虚端口”有很大不同。

1． 驱动机制不同

PPTP/L2TP 的虚端口是由路由表，通过 IP 路由匹配方式驱动的，无法根据业务类型创建不同的虚端口；而 IPSec 的端口是由“安全策略”驱动的。比如，同样是发送到公司总部的数据（目的 IP 地址相同），他们会通过相同的路由到达目的地，但是我们可以使用 IPSec 对其中的一些数据（如 EMAIL 数据）加密，对另外一些数据（如 HTTP）则不加密。

*WEB UI 方式下，在 **VPN 配置—>IPSec** 的“高级选项”中，可通过配置“筛选条件”下的“协议”和“端口”来配置业务策略（章节 6.1.1）。*

2． 生成方式不同

用户一旦正确配置了一条 PPTP/L2TP 隧道的相关参数，HiPER 系统会使用该配置自动生成一个“ptp”类型的虚端口用来传输数据，同时 IP 路由表里增加一条对应的 IP 路由条目（可以通过 *show ip route table* 看到，详见章节 2.2.2 或章节 3.2.2）。但是 IPSec 的策略是增加到系统“安全策略库”中的，用户配置了一条 IPSec 安全策略，该策略就被加入策略库，当有数据包需要发送时，系统就会把该数据包与安全策略库中的规则匹配，一旦有规则匹配该数据包，就对该数据包进行加密认证处理，然后再发送出去；当系统收到外部的一个进入包时，首先匹配安全策略库，看该数据包是否需要解密，然后才能进行正常的 IP 路由处理。

在 CLI 方式中，可以使用命令 ***show crypt ipsec sp*** *查看加密策略是否建立，如图 4-4 所示，表示加密策略已经建立。*

```
   profile if_n     out_fi      in_fi              tunSrc            tunDst  H   M
-----------------------------------------------------------------------------------
    PPPOE1     4     to_bjO     to_bjl      218.80.111.98    221.216.15.158  Y   N


--More Detail--
    out_fi    mtu  a_rly    nat_t  kp_ali  udp_e    dport  dpd_hb  dpd_to   dpd_a
-----------------------------------------------------------------------------------
    to_bjO  1450       N        Y      20      N        0       0       0       0
found 1 items in eroute table!
```

图 4-4 IPSec SP 建立信息

3．触发方式不同

PPTP/L2TP 虚端口由 IP 路由触发，IPSec 虚端口由系统安全策略库触发。接收处理时，安全策略在 IP 路由之前处理；当发送处理时，安全策略在 IP 路由之后处理。因此，根据触发的先后顺序不同，可以在 HiPER 上实现 IPSec Over PPTP/L2TP，或者 PPTP/L2TP Over IPSec 的应用，提供最高强度的 VPN 功能。

当收到第一个需要加密处理的数据包时，IPSec 会尝试与通信的对方发出建立 IPSec SA 的请求，建立了 IPSec SA 后，用户数据就可通过该隧道发送到对端网络设备上，对端设备把数据解密处理后发送到接收者所在的内网上。

在 CLI 方式中，可以使用命令 ***show crypt ipsec sa*** *查看 IPSec 是否建立，如图 4-5 所示，显示出信息"total：1 SA s active！"表示对应 IPSec SA 已经建立。*

```
… …
total:  1 SAs active!
```

图 4-5 IPSec SA 建立信息

提示：

在"野蛮方式"下，虽然 IPSec 中的"响应方"中配置了安全虚端口，但该端口只能工作在"监听"状态下，即使有数据需要向对方发送，也不会主动发起 IPSec SA 建立隧道的请求，这是因为通信对方的 IP 地址通常都是变化的，无法确定它的地址，也就无法发起呼叫请求建立隧道。

4.2.2.1 IPSec 发起方数据流

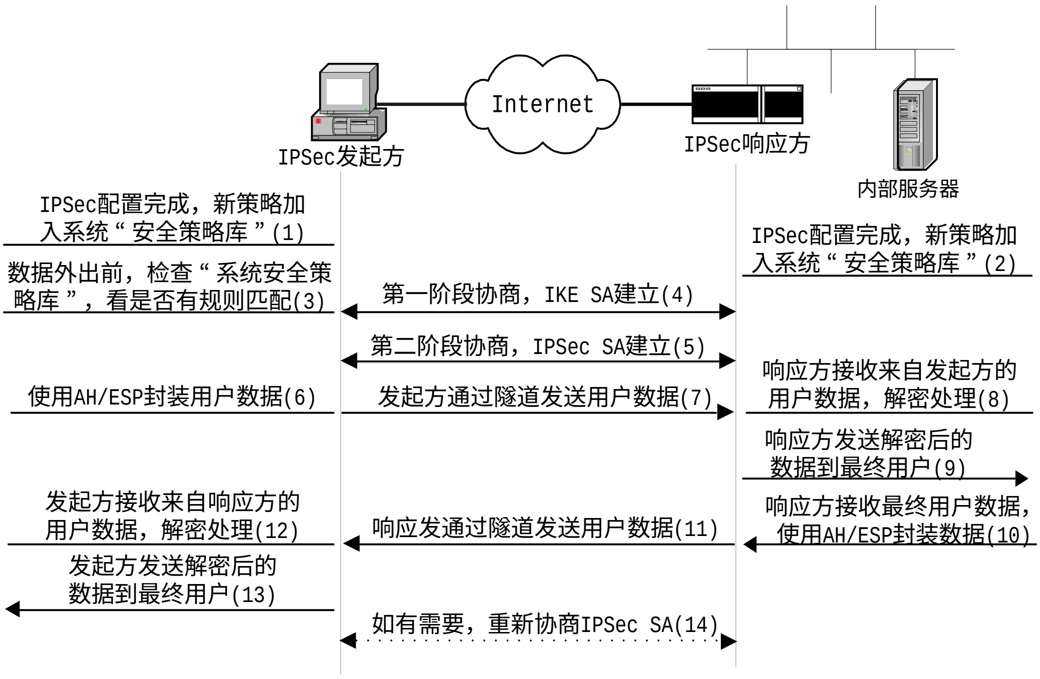


图 4-6 IPSec 隧道数据流

如图 4-6 所示，为“自动”方式下，IPSec 隧道建立及通过隧道传输数据的过程。在整个过程中，IPSec 发起方将依次通过以下数据流：

- 隧道配置完成，新策略加入系统“安全策略库”(图中（1)）；
- 数据外出前，检查“系统安全策略库”，看是否有规则（包括 IP 地址、协议和端口）匹配（图中（3)）；
- 第一阶段协商（由发起方发起），IKE SA 建立（图中（4)）；
- 第二阶段协商，IPSec SA 建立（图中（5)），参考章节 4.2.1.3；
- 发起方使用 AH/ESP 封装用户数据（图中（6)）；
- 发起方通过隧道发送用户数据（使用 AH/ESP 封装）（图中（7)）；
- 发起方接收来自响应方的用户数据（使用 AH/ESP 封装），解密处理（图中（12)）；
- 发送方发送解密后的数据到最终用户（图中（13)）；
- 如有需要，重新协商 IPSec SA（图中（14)，参考章节 4.2.1.4。

4.2.2.2 IPSec 响应方数据流

如图 4-6 所示，“自动”方式下，IPSec 隧道建立及数据传输的整个过程中，IPSec 响应方将依次通过以下数据流：

- 隧道配置完成，新策略加入系统“安全策略库”(图中（2)）；
- 第一阶段协商（由发起方发起），IKE SA 建立（图中（4)，参考章节 4.2.1.3）；
- 第二阶段协商，IPSec SA 建立（图中（5)）；
- 响应方接收来自发送方的用户数据（使用 AH/ESP 封装），解密处理（图中（8)）；
- 响应方发送解密后的数据到最终用户（图中（9)）；
- 响应方接收最终用户数据，使用 AH/ESP 封装用户数据（图中（10)）；

➢ 响应方通过隧道发送用户数据（使用 AH/ESP 封装）（图中（11））；
➢ 如有需要，重新协商 IPSec SA（图中（14）），参考章节 4.2.1.4。

提示：“手动”方式下，当正确配置完 IPSec 隧道参数后，SA 就自然建立了，因此这种情况下，没有 IKE 协商（两个阶段），其余的数据流同“自动”方式相同。

4.2.3 MTU 与分段数据传输

IPSec 协议在工作过程中使用了数据封装技术，当用户数据包本身比较大的时候(如 ERP 软件和 FTP 通常会使用比较大的数据包传输数据，MSN/QQ 等聊天软件发送的数据包比较小)，封装后的数据可能会超过发送物理端口最大发送单元 MTU (例如以太网接口的最大发送单元 MTU 是 1500 字节，超过 1500 字节大小的数据包将被强制分成多个数据包发送，以确保每个数据包可以被物理端口正确发送)，此时数据只能分段传输。在接收侧，收到分段后的数据必须组装还原为原来的数据包以后才能进行下一步协议处理，在接收到最后一个分段之前该数据包一直处在待处理状态。如果中间有一个分段丢弃，则整个数据包都被丢弃。

数据分段传输会严重影响系统的性能，所以传输过程中的再分段传输应当尽量避免。为解决此问题，HiPER IPSec 实现允许用户设置 MTU 的大小，尽量减少分段的可能性。

HiPER 中通过设置 IPSec 隧道的 MTU 参数来调整发送包的大小，超过该 MTU 大小的数据包会主动分段然后再发送。

CLI 方式中，可以使用命令 set ipsec config/xxx mtu 设置隧道的 MTU。
WEBUI 方式中，无此功能。

下面给出 IPSec 隧道的 MTU 的计算实例：

如图 4-7 和图 4-8 所示，为固定接入和 PPPoE 拨号时，IPSec 隧道中传输的封装数据包格式（以通道模式为例）。其中以太网 MTU 及各封装包头大小分别为：

以太网 MTU： 1500 字节；
IP 包头： 20 字节；
AH 包头（最大）： 20 字节；
ESP 包头（最大）： 40 字节；
PPPoE 包头： 8 字节；

IP 包头	AH 包头	ESP 包头	原始IP数据包

图 4-7 IPSec 隧道数据包格式（固定 IP 接入）

PPPoE 包头	IP 包头	AH 包头	ESP 包头	原始IP数据包

图 4-8 IPSec 隧道数据包格式（PPPoE 拨号）

因此，固定 IP 接入时（如图 4-7 所示），最大 MTU 不能大于 l420=1500-20-20-40，单位为字节；如果中间使用 PPPoE 线路（如图 4-8 所示），还要减去 PPPoE 的包头（8 字节），不能大于 1412=1420-8，单位为字节。

HiPER 中缺省的 IPSec 隧道的 MTU 是 1400，可以满足绝大部分应用的要求，一般无须修改。

4.3 IPSec NAT 穿透

由于历史的原因，部署 NAT 模式下的 IPSec VPN 网络的问题之一在于无法定位网络地址转换（NAT）之后的 IPSec 对话方。Internet 服务提供商和小型办公/家庭办公（SOHO）网络通常使用 NAT 共享单个公共 IP 地址。虽然 NAT 有助于节省剩余的 IP 地址空间，但是它们也给诸如 IPSec 之类的端对端协议带来了问题。

在 NAT 对 IPSec 造成中断的众多原因中，主要的一个原因就是，对于 " 封装安全性协议（ESP）" 来说，NAT 设备不能识别端口转换的 Layer 4（第 4 层）包头的位置（因为它已被加密）。对于 " 认证包头（AH）" 协议来说，NAT 设备能修改端口号，但不能修改认证检查，于是对整个 IPSec 封包的认证检查就会失败。

一种称为 IPSec NAT 穿透（NAT-T）的新技术正在由 Internet 工程任务组的 IPSec 网络工作组标准化。IPSec NAT-T 是在标题为 " IPSec 包的 UDP 封装 "（draft-ietf-ipsec-udp-encaps-02.txt）和" IKE 中的 NAT 穿越协商 "（draft-ietf-ipsec-nat-t-ike-02.txt）的 Internet 草案中描述的。IPSec NAT-T 对协商过程进行了修改，并且定义了发送受 IPSec 保护的数据的不同方法。

在 IPSec 协商过程中，可根据以下两个条件自动确定支持 IPSec NAT-T 的对话双方：

- 发起 IPSec 对话的一方（通常是一个客户端计算机）和响应 IPSec 对话的一方（通常是一个服务器）是否都能执行 IPSec NAT-T；
- 它们之间的路径中是否存在任何 NAT。

如果这两个条件同时为真，那么双方将使用 IPSec NAT-T 来通过 NAT 发送受 IPSec 保护的流量。如果其中一方不支持 IPSec NAT-T，则执行常规的 IPSec 协商（在前两个消息之后）和 IPSec 保护。如果双方都支持 IPSec NAT-T，但是它们之间不存在 NAT，则执行常规的 IPSec 保护。

提示：IPSec NAT-T 是仅为 ESP 流量定义的，AH 流量无法穿过 NAT 设备。

HiPER 设备可以应用 NAT 穿透 (NAT-T) 功能。NAT-T 在第一阶段交换过程中，沿着数据路径检测发现存在一个或多个 NAT 设备后，将添加一层 UDP 封装（通常使用 UDP4500 端口），从而通过 NAT 设备。

*WEB UI 方式下，在 **VPN 配置—>IPSec** 的 " 高级选项 " 中，可通过选中 "NAT 穿透 " 选项来启用 NAT 穿透功能（章节 6.1.1）。*

4.4 IPSec 会话数量限制

针对不同的产品型号，HiPER 中支持 IPSec VPN 隧道的会话数量是不一样的。IPSec 会话数量根据具体的产品规格说明书确定，超过系统支持能力的会话将拒绝。当 VPN 会话数已达最大值时，如果尝试建立新的会话，系统会显示如下信息：



图 4-9 对话框 — VPN 会话数达到最大

CLI 方式中，可使用命令 show session history 查看相关信息，如图 4-9 所示，有“Max VPN sessions。Cannot set up a new IPSec session。”相关信息显示，无法再建立新的 IPSec 会话。

*WEBUI 方式中，可在**系统状态—>系统信息**的“系统历史记录”中查看相关信息。如图 4-10 所示，在系统历史记录中有“Max VPN sessions。Cannot set up a new IPSec session。”相关信息显示，无法再建立新的 IPSec 会话。*

```
04:13:18        Max VPN sessions.Cannot set up a new IPSec session.
04:13:15        Ethernet Up
```

图 4-10 CLI 中无法建立新的 IPSec 会话信息

```
04:13:18 Max VPN sessions.Cannot set up a new IPSec session.
04:13:15 Ethernet Up
```

图 4-11 WEBUI 中无法建立新的 IPSec 会话信息

4.5 小结

IPSec VPN 协议提供了较高的安全等级，能够满足大多数公司的安全需要。同 PPTP/L2TP 以及其它的 VPN 解决方案相比，尽管 IPSec 具有更高的安全性，但是它的部署通常更加昂贵，配置更加复杂，而且受到一定的限制（如 NAT 设备，IP 地址变化等）。

4.6 协议标准及参考资料

HiPER 中 IPSec 的实现遵循以下标准：

RFC2401 Security Architecture for the Internet Protocol，IP 层协议安全体系结构

RFC2407 The Intenet IP Security Domain of Interpretation for ISAKMP，用于因特网安全联盟和密钥管理协议（ISAKMP）的 IP 安全解释域

RFC2408 Internet Security Assocation and Key Management Protocol（ISAKMP），因特网安全联盟和密钥管理协议

RFC2409 The Internet Key Exchange（IKE），因特网密钥交换

第5章 HiPER PPTP 和 L2TP 配置

5.1 PPTP 和 L2TP 配置界面

HiPER VPN 网关可以工作在 PPTP/L2TP 客户端的模式下，也可以工作在 PPTP/L2TP 服务器的模式下。当 HiPER 作为 PPTP/L2TP 客户端使用时（如图 5-1），将“业务类型”选择为“拨出（客户端）”；当 HiPER 作为 PPTP/L2TP 服务器使用时（如图 5-3），将“业务类型”选择为“拨入（服务器）”。

5.1.1 PPTP/L2TP 客户端的配置参数



图 5-1 PPTP/L2TP 客户端配置界面

- 设置名：PPTP/L2TP 隧道的名称（自定义，不可重复，不能超过 31 个字符）；
- 业务类型：拨出（客户端），HiPER 作为 PPTP/L2TP 隧道连接的发起者，拨号到远端 PPTP/L2TP 服务器；
- 用户名：PPTP/L2TP 隧道的用户名；
- 协议类型：

  L2TP：本地客户端将使用 L2TP 协议和对端服务器协商创建 L2TP 隧道；

  PPTP：本地客户端将使用 PPTP 协议和对端服务器协商创建 PPTP 隧道；
- 密码：PPTP/L2TP 隧道的用户密码；

- 确认密码：PPTP/L2TP 隧道的用户密码（此处必须和上一栏所填密码一致）；
- 密码验证方式：PPTP/L2TP 隧道的密码验证方式，选项：PAP，CHAP，MS-CHAP，NONE（不验证）；
- 远端内网 IP 地址：PPTP/L2TP 隧道对端局域网所使用的 IP 地址（一般可以填 PPTP/L2TP 隧道对端设备的 LAN 口 IP 地址）；
- 远端内网子网掩码：PPTP/L2TP 隧道对端局域网所使用的子网掩码；
- 隧道服务器地址（名）：PPTP/L2TP 服务器的 IP 地址或者域名（一般填 PPTP/L2TP 隧道对端设备的 WAN 口 IP 地址或域名）。

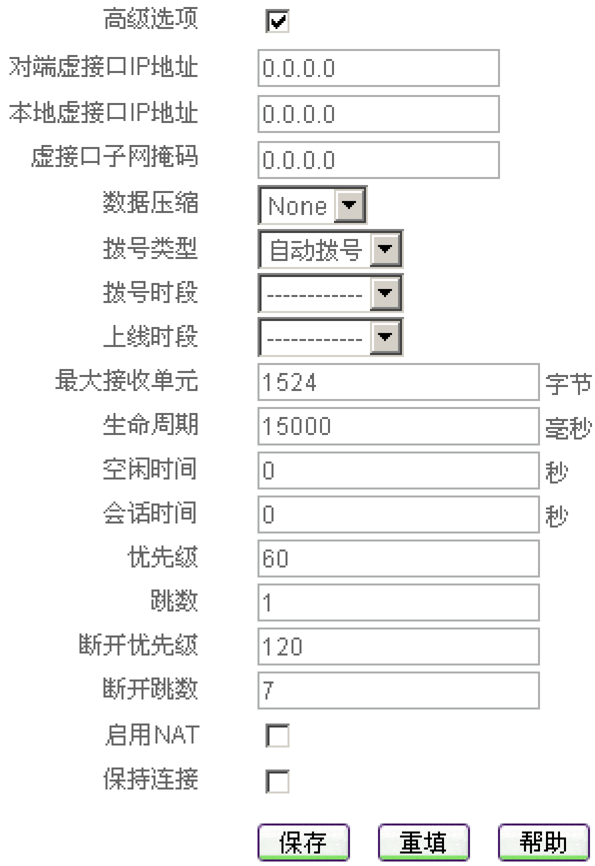


图 5-2 PPTP/L2TP 客户端配置界面（高级选项）

- 高级选项：选中后显示 PPTP/L2TP 隧道的高级配置参数；
- 对端虚接口 IP 地址：对端设备虚接口的 IP 地址（一般情况下无需设置）；
- 本地虚接口 IP 地址：本地设备虚接口的 IP 地址（一般情况下无需设置）；
- 虚接口子网掩码：PPTP/L2TP 隧道两端设备虚接口的子网掩码（一般情况下无需设置）；
- 数据压缩：选择数据压缩类型，选项：NONE，没有数据压缩；Stac9，PPP 层上启用 Stac9 压缩（必须 PPTP/L2TP 隧道对端设备启用了相同配置才可使用）；
- 拨号类型：

  自动拨号：当参数配置完成，或上一次 PPTP/L2TP 隧道连接中断，或开启 HiPER VPN 网关时，PPTP/L2TP 客户端将自动拨号（发起建立隧道请求）；

  手动拨号：在 ***VPN 配置—>PPTP 和 L2TP***（章节 5.1.3）中，手工进行连接和挂断 PPTP/L2TP 隧道；

  按需拨号：参数配置完成后，一旦 PPTP/L2TP 客户端监听到有用户数据需要传输，就拨号（发起建立隧道请求）；

- 拨号时段：允许 PPTP/L2TP 客户端拨号（发起建立隧道请求）的时间段（时间段在***基本配置—>时间段配置***中定义），只有在此时间段范围内才允许 PPTP/L2TP 客户端触发拨号，不设置代表不对拨号时段进行控制；
- 上线时段：允许 PPTP/L2TP 客户端保持 PPTP/L2TP 隧道连接的时间段（时间段在***基本配置—>时间段配置***中定义），HiPER 安全网关在超出这个时间段的时间后会自动断开 PPTP/L2TP 隧道连接，不设置代表不对上线时段进行控制；
- 最大接收单元：PPTP/L2TP 隧道两端允许通过的最大数据包长度，缺省值为 1524 字节，VPN 拨号时 HiPER 将自动与对方设备协商，除非特别应用，不要修改；
- 保持连接/生命周期：选中 " 保持连接 " 后，从 PPTP/L2TP 隧道连接成功开始，系统会每隔 1000ms 向对端网络设备发送一个探测包，以探测隧道连接是否正常，如果在 " 生命周期 "（默认值：15000 毫秒）范围内一直没有收到对方回应，则断开此连接。一般情况下无需设置，系统会发送 PPTP/L2TP 隧道默认的 HELLO 数据包来探测隧道连接是否正常；
- 空闲时间：在没有访问流量后自动断线前等待的时长，当 PPTP/L2TP 隧道连接成功后，如果隧道空闲（没有数据传输）的时间超过了预设的" 空闲时间 "，HiPER VPN 网关将主动断开连接，0 代表不自动断线（单位：秒）；
- 会话时间：设置连接生存时间（一般情况下不要设置），一旦隧道连接的时间（从拨号成功开始）超出了 " 会话时间 "，HiPER 会自动挂断隧道连接，0 代表没有时间限制（单位：秒）；
- 优先级：拨号成功后，该线路的路由优先级，目的网段相同的情况下，HiPER 将优先选择优先级高的线路转发数据包，值越低优先级越高；
- 跳数：拨号成功后，该线路的路由跳数，从源到目的的路径中每一跳被赋以一个跳数值，此值通常为 1；跳数也表示该条路由记录的质量，一般情况下，如果有多条到达相同目的地的路由记录，HiPER 会采用跳数值小的那条路由；
- 断开优先级：PPTP/L2TP 隧道连接中断后，该线路的路由优先级，优先级高的优先拨号，值越低优先级越高；
- 断开跳数：PPTP/L2TP 隧道连接中断后，该线路的路由跳数；
- 启用 NAT：开启此项功能后，PPTP/L2TP 客户端会对此 PPTP/L2TP 隧道连接进行 NAT，即将局域网用户的 IP 地址转化为对端 PPTP/L2TP 服务器分配的 IP 地址，这样局域网用户将使用 PPTP/L2TP 服务器分配的 IP 地址连接到隧道对端的局域网，隧道对端设备无需设置到本地的路由。但是这种情况下只能实现本地网络到隧道对端网络的单向访问（适合 HiPER 使用移动用户的帐号连接到 PPTP/L2TP 服务器）；

- 保存：PPTP/L2TP 客户端配置参数生效；
- 重填：恢复到修改前的配置参数。

5.1.2 PPTP/L2TP 服务器的配置参数



图 5-3 PPTP/L2TP 服务器配置界面

- 设置名：PPTP/L2TP 隧道的名称（自定义，不可重复，不能超过 31 个字符），此名称同时作为 PPTP/L2TP 客户端的用户名；
- 业务类型：拨入（服务器），HiPER 作为 PPTP/L2TP 隧道连接的终结者，接收来自 PPTP/L2TP 客户端的拨入；
- 用户类型：

  LAN 到 LAN：拨入的 PPTP/L2TP 用户是一个网段的用户，往往是通过一个路由器拨入，实现 PPTP/L2TP 隧道两端局域网的通信；

  移动用户：拨入的 VPN 用户是个人用户，往往由单个计算机拨入，实现 PPTP/L2TP 隧道远端计算机与本地局域网的通信；
- 密码：PPTP/L2TP 隧道的用户密码；
- 确认密码：PPTP/L2TP 隧道的用户密码（此处和上一栏所填密码一致）；
- 密码验证方式：PPTP/L2TP 隧道的用户密码验证方式，选项：PAP，CHAP，MS-CHAP，NONE（不验证）；
- 远端内网 IP 地址：PPTP/L2TP 隧道对端局域网所使用的 IP 地址（一般可以填 VPN 隧道对端设备的 LAN 口 IP 地址），当拨入用户类型选择为“移动用户”时系统会自动生成；
- 远端内网子网掩码：PPTP/L2TP 隧道对端局域网所使用的子网掩码，当拨入用户类型为“移动用户”时系统会自动生成；
- 分配 IP 地址：PPTP/L2TP 服务器要从 VPN 地址池取出一个 IP 地址分配给拨入的用户，作为连接 PPTP/L2TP 隧道两端的路由地址，选中后，即可为拨入的用户分配

IP 地址。注意，所有拨入用户共享一个地址池；

- 地址池开始地址：设置 VPN 地址池开始地址（可以是任意网段的 IP 地址，但是不能和整个 VPN 方案中已有的任何 IP 地址段重复）；
- 地址池地址数：设置 VPN 地址池的地址数量。

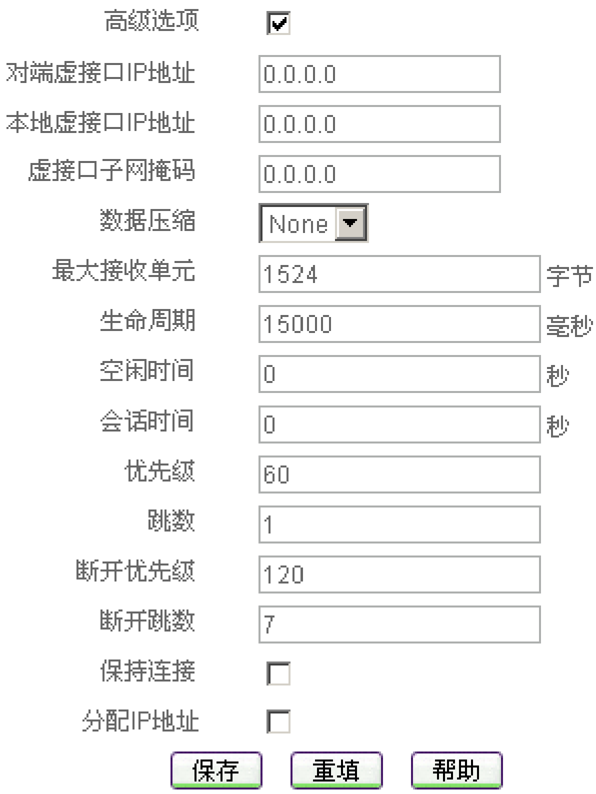


图 5-4　PPTP/L2TP 服务器配置界面（高级选项）

- 高级选项：选中后显示 PPTP/L2TP 隧道的高级配置参数；
- 对端虚接口 IP 地址：对端设备虚接口的 IP 地址（一般情况下无需设置）；
- 本地虚接口 IP 地址：本地设备虚接口的 IP 地址（一般情况下无需设置）；
- 虚接口子网掩码：PPTP/L2TP 隧道两端设备虚接口的子网掩码（一般情况下无需设置）；
- 数据压缩：选择数据压缩类型，选项：NONE，没有数据压缩；Stac9，PPP 层上启用 Stac9 压缩（必须 PPTP/L2TP 隧道对端设备启用了相同配置才可使用）；
- 最大接收单元：PPTP/L2TP 隧道两端允许通过的最大数据包长度，缺省值为 1524 字节，VPN 拨号时 HiPER 将自动与对方设备协商，除非特别应用，不要修改；
- 保持连接/生命周期：选中“保持连接”后，从 PPTP/L2TP 隧道连接成功开始，系统会每隔 1000ms 向对端网络设备发送一个探测包，以探测隧道连接是否正常，如果在“生命周期”（默认值：15000 毫秒）范围内一直没有收到对方回应，则断开此连接。一般情况下无需设置，系统会发送 PPTP/L2TP 隧道默认的 HELLO 数据包来探测隧道连接是否正常；
- 空闲时间：在没有访问流量后自动断线前等待的时长，当 PPTP/L2TP 隧道连接成功后，如果隧道空闲（没有数据传输）的时间超过了预设的“空闲时间”，HiPER VPN 网关将主动断开连接，0 代表不自动断线（单位：秒）；
- 会话时间：设置连接生存时间（一般情况下不要设置），一旦隧道连接的时间（从拨号成功开始）超出了“会话时间”，HiPER VPN 网关会自动挂断隧道连接，0 代

表没有时间限制（单位：秒）；

- 优先级：拨号成功后，该线路的路由优先级，目的网段相同的情况下，HiPER 将优先选择优先级高的线路转发数据包，值越低优先级越高；
- 跳数：拨号成功后，该线路的路由跳数，从源到目的的路径中每一跳被赋以一个跳数值，此值通常为 1；跳数也表示该条路由记录的质量，一般情况下，如果有多条到达相同目的地的路由记录，HiPER 会采用跳数值小的那条路由；
- 断开优先级：PPTP/L2TP 隧道连接中断后，该线路的路由优先级，优先级高的优先拨号，值越低优先级越高；
- 断开跳数：PPTP/L2TP 隧道连接中断后，该线路的路由跳数；
- 保存：PPTP/L2TP 客户端配置参数生效；
- 重填：恢复到修改前的配置参数。

5.1.3 配置 PPTP/L2TP 客户端和服务器的注意事项

1. 当 PPTP/L2TP 隧道两端设备建立连接时，会各用一个虚接口来连接对方。一般情况下，PPTP/L2TP 服务器会从地址池分配一个 IP 地址作为两个虚接口的路由地址；但是某些 PPTP/L2TP 服务器并没有配置地址池，此时需要为隧道两端设备的虚接口配置 IP 地址来作为各自的路由地址，即配置"对端虚接口 IP 地址"、"本地虚接口 IP 地址"及"虚接口子网掩码"这三个参数。注意，PPTP/L2TP 隧道两端设备虚接口使用同一个子网掩码。

2. L2TP 协议使用 UDP 1701 端口传输数据，PPTP 协议使用 TCP 1723 端口建立连接。为保证 HiPER 启用 NAT 后，PPTP/L2TP 隧道正常连接，在配置 PPTP/L2TP 后，系统会自动生成一条 UDP 1701 端口、TCP 1723 端口的 NAT 静态映射（***高级配置—>NAT 和 DMZ 配置***的"NAT 静态映射列表"中名称为"l2tp"、"pptp"的 NAT 静态映射）。请不要编辑、删除它们，否则可能造成 PPTP/L2TP 隧道无法连接和传输数据。

5.1.4 PPTP/L2TP 信息列表



表 5-1 PPTP/L2TP 信息列表



表 5-2 PPTP/L2TP 信息列表（续表 5-1）

一旦 PPTP/L2TP 隧道的配置完成提交以后，即可在 ***VPN 配置—>PPTP 和 L2TP*** 页面的“ PPTP/L2TP 信息列表 ”（如表 5-1、表 5-2 所示）中查看已建立的 PPTP/L2TP 隧道的配置及状态信息，各参数含义解释如下：

- 设置名：PPTP/L2TP 隧道的名称；
- 用户名：PPTP/L2TP 隧道的用户名；
- 允许：是否启用当前 PPTP/L2TP 实例。选中表示启用；不选中表示禁用当前 PPTP/L2TP 实例，相关配置保留但不生效；
- 会话状态：PPTP/L2TP 隧道的当前连接状态，共有 7 种状态，详见表 5-3；

状态	描述
关闭	隧道处于未连接状态
拨号中	正在尝试 VPN 拨出或者是正在尝试接收 VPN 拨入
验证中	正在进行用户验证（L2TP 还包括隧道验证）
已连接	验证成功，隧道连接已建立
断线中	正在拆除隧道连接
已挂机	一方已发出挂机请求
已断线	隧道连接已中断，等待拨号

表 5-3 PPTP/L2TP 隧道连接状态

- 远端网关：业务类型为“ VPN 拨出 ”时，该值为配置 PPTP/L2TP 客户端时填写的“ 隧道服务器地址（名）”；业务类型为“ VPN 拨入 ”时，该值为拨入的 PPTP/L2TP 客户端的外网 IP 地址；
- 远端内网 IP 地址：配置 PPTP/L2TP 客户端或服务器时填写的“ 远端内网 IP 地址 ”；
- 使用时间：PPTP/L2TP 隧道连接成功至查看时刻的时间；
- 空闲时间：用户最后一次使用 PPTP/L2TP 隧道传输数据至查看时刻的时间；
- 出流量：通过 PPTP/L2TP 隧道发出的数据包的统计数量（单位：字节）；
- 入流量：通过 PPTP/L2TP 隧道接收的数据包的统计数量（单位：字节）；
- 业务类型：该端的业务类型，该值为“ VPN 拨出 ”或“ VPN 拨入 ”；
- 协议类型：PPTP/L2TP 隧道使用的协议类型：“ L2TP ” 或 “ PPTP ”。当隧道处于未

连接状态时，PPTP/L2TP 服务器中显示的是“ PPTP&L2TP ”；

- 虚接口地址：虚接口的 IP 地址，当 PPTP/L2TP 隧道两端设备建立连接时，会各用一个虚端口来连接对方。业务类型为“ VPN 拨出 ”时，该值为 PPTP/L2TP 服务器分配的 IP 地址（连接成功前显示为“ 0.0.0.0 ”）；业务类型为“ VPN 拨入 ”时，该值为分配给 PPTP/L2TP 客户端的 IP 地址（连接成功前显示为“ 255.255.255.255 ”）；
- 是否加密：PPTP/L2TP 隧道是否使用 MPPE 加密；
- 导出 WINDOWS 注册表文件：缺省的 Windows 2000/XP L2TP 传输策略不允许 L2TP 传输不使用 IPSec 加密，可以通过修改 Windows 2000/XP 注册表来禁用缺省的行为。单击“ 导出 WINDOWS 注册表文件 ”超链接，即可导出并保存 WINODWS 注册表文件（文件名为“ l2tp.reg ”）到主机，运行该文件后即可修改注册表，修改后重启电脑以使改动生效；
- 建立：选中某条 PPTP/L2TP 隧道，单击“ 建立 ”按钮，即可通过手动的方式建立该条 PPTP/L2TP 隧道的连接（仅在业务类型是拨出时可用）；
- 挂断：选中某条 PPTP/L2TP 隧道，单击“ 挂断 ”按钮，即可通过手动的方式挂断该条 PPTP/L2TP 隧道的连接；
- 刷新：单击“ 刷新 ”，可以显示最新的“ PPTP/L2TP 信息列表 ”。

5.1.5 PPTP/L2TP 隧道的拨号与挂断

在 PPTP/L2TP 隧道建立连接的过程中，只能由“ 拨出 ”方（PPTP/L2TP 客户端）发起建立隧道请求。PPTP/L2TP 隧道的拨号方式由 PPTP/L2TP 客户端配置的“ 拨号类型 ”来确定。

1. 如果“ 拨号类型 ”选择为“ 自动拨号 ”（推荐使用），配置完成后 PPTP/L2TP 客户端会自动向 PPTP/L2TP 服务器发起建立隧道请求，直至 PPTP/L2TP 隧道连接成功为止。一旦隧道连接中断，PPTP/L2TP 客户端就会自动拨号，发起建立隧道请求。
2. 如果“ 拨号类型 ”选择为“ 按需拨号 ”，配置完成后，一旦 PPTP/L2TP 客户端监听到有用户数据需要传输时，就拨号，发起建立隧道请求（参见章节 2.2.2）。同样，当隧道连接中断时，只有等到有用户数据需要传输时，PPTP/L2TP 客户端才会拨号。
3. 如果“ 拨号类型 ”选择为“ 手动拨号 ”，配置完成后，必须通过手动建立连接，才能使 PPTP/L2TP 客户端发起建立 PPTP/L2TP 隧道请求（参见章节 5.1.3）。同样，当隧道连接中断时，只有通过手动促使 PPTP/L2TP 客户端拨号。

当 PPTP/L2TP 隧道连接成功后，如果隧道连接中断，正常情况下存在以下几种可能性。

1. PPTP/L2TP 隧道连接成功后，HiPER 会发送 PPTP/L2TP 隧道默认的 HELLO 数据包来探测连接是否正常，如果没有收到隧道对端回应的 HELLO 数据包，HiPER 将会自动挂断隧道连接。
2. 如果配置了“ 保持连接 ”，系统还会每隔 1000ms 向对端发送探测包来判断连接是否正常，如果在“ 生命周期 ”内一直没有收到对方回应的数据包，HiPER 也会自动挂断隧道连接。
3. 当 PPTP/L2TP 隧道连接成功后，如果隧道空闲（没有数据传输）的时间超过了预设的“ 空闲时间 ”，HiPER 关将主动断开连接（参见章节 2.2.2）。
4. 如果配置了“ 会话时间 ”，一旦隧道连接的时间（从拨号成功开始）超出了“ 会话时间 ”，HiPER 安全网关会自动挂断隧道连接。
5. 如果用户主动拆除隧道（手动挂断），PPTP/L2TP 隧道将断开。

提示：

1. 当 HiPER 安全网关作为 PPTP/L2TP 客户端使用时，如果设置了“拨号时段”，那么只有在设置的“拨号时段”时间范围内才允许 HiPER 拨号，发起建立隧道请求。
2. 当 HiPER 安全网关作为 PPTP/L2TP 客户端使用时，如果设置了“上线时段”，那么在超出这个时间段的时间后 HiPER 会自动挂断隧道连接。

5.1.6 PPTP/L2TP 隧道的增加、浏览、编辑与删除

- 增加 PPTP/L2TP 隧道：选中“添加”选项，输入 PPTP/L2TP 隧道信息，再单击“保存”按钮，就生成新的 PPTP/L2TP 隧道，如图 5-1~图 5-4 所示；
- 浏览 PPTP/L2TP 隧道：如果已经生成了 PPTP/L2TP 隧道，可以在“PPTP/L2TP 信息列表”中查看相关信息及状态，如表 5-1 所示；
- 编辑 PPTP/L2TP 隧道：如果想编辑某一 PPTP/L2TP 隧道，首先点击该 PPTP/L2TP 隧道的“设置名”超链接，该 PPTP/L2TP 隧道的信息将填充到相应的编辑框内，然后修改它，再单击“保存”按钮，修改完毕；
- 删除 PPTP/L2TP 隧道：只需选中一些 PPTP/L2TP 隧道（在最左边的方框中打“√”），单击左下角的“删除”按钮，即可删除那些被选中的 PPTP/L2TP 隧道。

5.1.7 PPTP/L2TP 隧道的历史纪录

在*系统状态—>系统信息*的“系统历史记录”中可以查看建立和挂断 PPTP/L2TP 隧道连接时，隧道两端的历史纪录（排列在系统历史记录最上面的一条消息为最新的一条消息），相关历史记录及含义如表 5-4 所示（这里以 L2TP 为例进行说明）：

	历史纪录	记录含义
L2TP 客户端（拨出端）	Session Up [X] L2tp Up 200.200.200.173 Call Connected , on Line 1, on Channel 0 Outgoing Call @0:1-1	某连接成功建立，[x]为 L2TP 隧道名 L2TP 成功和 IP 地址为 200.200.200.173 的设备建立连接 物理层/链路层连接完成，但 IP 仍不可用 连接开始呼出
	Call Terminated @clearSession:1 L2tp Up 200.200.200.173 Call Connected , on Line 1, on Channel 0 Outgoing Call @0:1-1	呼叫失败（用户名、密码、验证方式或者是其他 PPP 层错误） L2TP 成功和 IP 地址为 200.200.200.173 的设备建立连接 物理层/链路层连接完成，但 IP 仍不可用 连接开始呼出
	Call Terminated @clearSession:1 Outgoing Call @0:1-1	呼叫失败（找不到对端或者是对端无响应） 连接开始呼出
	Session down [x]	某连接挂断，[x]为 L2TP 隧道名

L2TP 服务器（拨入端）	Session Up [X] L2tp Up 200.200.200.176 Assigned to port Call Connected , on Line 1, on Channel 0 Incoming Call , on Line 1, on Channel 0	某连接成功建立，[x]为 L2TP 隧道名 L2TP 成功和 IP 地址为 200.200.200.176 的设备建立连接 协商成功，为拨入的连接分配虚端口 物理层/链路层连接完成，但 IP 仍不可用 有远端呼叫拨入
	Call Terminated @clearSession:1 Security error VPN_remote L2tp Up 200.200.200.176 Assigned to port Call Connected , on Line 1, on Channel 0 Incoming Call , on Line 1, on Channel 0	呼叫失败 安全层错误（用户名、密码、验证方式或者是其他 PPP 层错误） L2TP 成功和 IP 地址为 200.200.200.176 的设备建立连接 为拨入的连接分配虚端口 物理层/链路层连接完成，但 IP 仍不可用 有远端呼叫拨入
	Session down [x]	某连接挂断，[x]为 L2TP 隧道名

表 5-4 L2TP 隧道的历史记录

5.1.8 路由表

在*系统状态—>路由和端口信息*的“路由表信息列表”中可以查看建立 PPTP/L2TP 隧道连接前后，PPTP/L2TP 客户端或 PPTP/L2TP 服务器的虚端口和相关路由的状态信息（参见章节 2.2.2 及章节 3.2.2），相关信息及描述如表 5-5 所示。

	状态	路由表						
PPTP/L2TP 客户端	拨出前	192.168.123.0/24	192.168.123.1	ptpdial0	luga	120	7	0
		192.168.123.1/32	192.168.123.1	ptpdial0	luha	120	7	1
		到目的地址“192.168.123.0/24”的 PPTP/L2TP 隧道连接未成功，路由虚端口未被激活（ptpdial0），网关地址为预设的“远端内网 IP 地址”。						
	拨出成功后	192.168.123.0/24	10.10.10.14	ptp4	lug	60	1	0
		192.168.123.1/32	10.10.10.14	ptp4	lugh	60	1	0
		到目的地址“192.168.123.0/24”的 PPTP/L2TP 隧道连接已成功，路由虚端口被激活（ptp4），网关地址是 PPTP/L2TP 服务器分配的 IP 地址（10.10.10.14/32）。						
PPTP/L2TP 服务器	拨入前	192.168.16.0/24	192.168.16.1	ptpdial0	luga	120	7	0
		192.168.16.1/32	192.168.16.1	ptpdial0	luha	120	7	1
		到目的地址“192.168.16.0/24”的 PPTP/L2TP 隧道连接未成功，路由虚端口未被激活（ptpdial0），网关地址为预设的“远端内网 IP 地址”。						

	拨入成功后	0.0.0.0/0	200.200.200.172	ie1	lugpaN	60	1	0
		10.10.10.14/32	10.10.10.14	ptp7	Ruht	60	1	0
		127.0.0.0/8	-	bhole0	cup	20	0	0
		127.0.0.1/32	-	local	cuhp	20	0	0
		127.0.0.2/32	-	reject0	cuhp	20	0	0
		127.0.0.3/32	-	bhole0	cuhp	20	0	0
		192.1.2.0/24	-	ie0	cua	20	0	4
		192.1.2.1/32	-	local	cuhp	20	0	0
		192.168.16.0/24	10.10.10.14	ptp7	lug	60	1	0
		192.168.16.1/32	10.10.10.14	ptp7	lugh	60	1	0
		到目的地址“ 192.168.16.0/24 ”的 PPTP/L2TP 隧道连接已经成功，路由虚端口被激活（ptp7），网关地址为分配给 PPTP/L2TP 客户端的 IP 地址（10.10.10.14/32）。						

表 5-5 PPTP/L2TP 隧道的路由信息

5.2 L2TP 配置实例

5.2.1 配置 HiPER 作为 L2TP 服务器

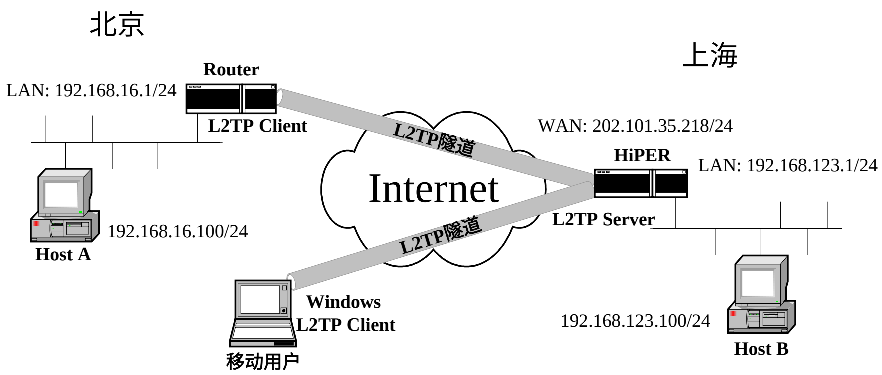


图 5-5 方案——HiPER 作为 L2TP 服务器

在本方案中，某公司总部在上海。在北京有一个分公司希望可以实现两地局域网内部资源的相互访问。该公司还有一些出差和远程办公的移动用户希望在远程访问总公司局域网内部资源。

本方案使用 L2TP 协议建立 VPN 隧道，如图 5-5 所示，在上海公司总部使用 HiPER VPN 网关作为 L2TP 服务器，在北京放置任意品牌的标准 VPN 路由器（推荐使用 HiPER VPN 网关）作为 L2TP 客户端，移动用户使用 Windows 操作系统内置的 L2TP 客户端软件。地址如下：

上海的 HiPER：

局域网网段 IP 地址：192.168.123.0/24

HiPER 的 LAN 口 IP 地址：192.168.123.1/24

HiPER 的 WAN 口 IP 地址：202.101.35.218/24

北京的路由器

局域网网段 IP 地址：192.168.16.0/24

路由器的 LAN 口 IP 地址：192.168.16.1/24

移动用户：

使用 Windows 操作系统通过 L2TP 拨号完成隧道连接。

5.2.1.1 配置 HiPER 作为 L2TP 服务器（LAN 到 LAN/移动用户拨入）

1. 为北京的路由器创建 L2TP 拨入帐号

在 ***VPN 配置—>PPTP 和 L2TP*** 中，选择 “ 添加 ” 选项，然后在配置参数项中依次输入以下内容，再单击 “ 保存 ” 按钮。

“ 设置名 ”：vpn_bj

“ 业务类型 ”：拨入（服务器）

“ 用户类型 ”：LAN 到 LAN

“ 密码 ”：vpntest

“ 确认密码 ”：vpntest

“ 密码验证方式 ”：PAP

“ 远端内网 IP 地址 ”：192.168.16.1（L2TP 隧道对端局域网所使用的 IP 地址）

“ 远端内网子网掩码 ”：255.255.255.0

“ 分配 IP 地址 ”：选中

“ 地址池开始地址 ”：10.10.10.10（不能和整个 VPN 方案中已有 IP 地址段重复）

“ 地址池地址数 ”：50

2. 为移动用户创建 L2TP 拨入帐号

在 ***VPN 配置—>PPTP 和 L2TP*** 中，选择 “ 添加 ” 选项，然后在配置参数项中依次输入以下内容，再单击 “ 保存 ” 按钮。

“ 设置名 ”：vpn_mobile

“ 业务类型 ”：拨入（服务器）

“ 用户类型 ”：移动用户

“ 密码 ”：vpntest

“ 确认密码 ”：vpntest

“ 密码验证方式 ”：PAP

“ 分配 IP 地址 ”：选中（同本节 1 中配置）

“ 地址池开始地址 ”：10.10.10.10（同本节 1 中配置）

“ 地址池地址数 ”：50（同本节 1 中配置）

5.2.1.2 配置 HiPER 作为 L2TP 客户端（LAN 到 LAN）

配置同章节 5.2.2.1（配置 HiPER 作为 L2TP 客户端）。

5.2.1.3 配置 Windows 2000 作为 L2TP 客户端（移动用户）

按照以下步骤配置 Windows 2000 计算机，使其成为 L2TP 客户端。

1. 配置 L2TP 拨号连接

1） 进入 Windows 2000 的“开始”→“设置”→“网络与拨号连接”→“新建连接”。
2） 启动“网络连接向导”，单击“下一步”。
3） 在“网络连接类型”中，选择“通过 Internet 连接到专用网络”，单击“下一步”。
4） 选择“不拨初始连接”，单击“下一步”。
5） 在“目的地址”一栏，输入准备连接的 L2TP 服务器的 IP 地址“202.101.35.218”，单击“下一步”。
6） 选择“只是我自己可以使用此连接”，单击“下一步”。
7） 输入“您为这个连接使用的名称”为“l2tp”。
8） 单击“完成”。
9） 双击“l2tp”连接，在 l2tp 连接窗口，单击“属性”。
10）进入“安全措施”属性页面，选择“高级（自定义设置）”，单击“设置”。
11）在“数据加密”中选择“可选加密（没有加密也可以连接）”。
12）在“允许这些协议”选中“不加密的密码（PAP）”、“质询握手身份验证协议（CHAP）”、“Microsoft CHAP（MS-CHAP）”，单击“确定”。
13）进入“网络”属性页面，在“我正在呼叫的 VPN 服务器的类型”选择“第 2 层隧道协议（L2TP）”。
14）单击“确定”，保存所做的修改。

2. 禁用 IPSec

1） 双击“l2tp”连接，在 l2tp 连接窗口，单击“属性”。
2） 选择“网络”属性页面。
3） 确认“NWLink IPX/SPX/NetBIOS Compatible Transport Prococol”协议没有被选中。
4） 选择“Internet 协议（TCP/IP）”，单击“属性”。
5） 单击“高级属性”属性页面。
6） 进入“选项”属性页面，选择“IP 安全机制”，单击“属性”。
7） 确认“不使用 IPSec”被选中。
8） 单击“确定”，关闭连接属性窗口。

3. 修改注册表

缺省的 Windows 2000 L2TP 传输策略不允许 L2TP 传输不使用 IPSec 加密，可以通过修改 Windows 2000 注册表来禁用缺省的行为。

方法一：单击“导出 WINDOWS 注册表文件”超链接，即可导出并保存 WINDOWS 注册表文件（文件名为“l2tp.reg”）到主机，运行该文件后即可修改注册表，改动后重启电脑以使改动生效。

方法二：手工修改：

1） 进入 Windows 2000 的“开始”→“运行”里面输入“Regedt32”，打开“注册表编辑器”，定位“HKEY_Local_Machine \ System \ CurrentControl Set \ Services \ RasMan \ Parameters ”主键。
2） 选择“编辑”→“添加数值”，为该主键添加以下键值：
   数值名称：ProhibitIpSec
   数据类型：reg_dword
   值：1
3） 保存所做的修改，重新启动电脑以使改动生效。

提示 必须添加“ProhibitIpSec”注册表键值到每个要使用 L2TP 的运行 Windows 2000 操作系统的电脑。

4. 使用 L2TP 隧道连接到 HiPER L2TP 服务器
   1） 确认计算机已经连接到 Internet（可能是拨号连接或者是固定 IP 接入）。
   2） 启动前面步骤中创建的“ l2tp ”拨号连接。
   3） 输入 l2tp 连接的用户名“ vpn_mobile ”和密码“ vpntest ”。
   4） 单击“ 连接 ”。
   5） 连接成功后，在 MS-DOS 方式下输入“ ipconfig ”，可以看到一个在 L2TP 服务器地址池中的地址，就是 L2TP 服务器分配给本机的 IP 地址。

5.2.1.4 配置 Windows XP 作为 L2TP 客户端（移动用户）

按照以下步骤配置 Windows XP 计算机，使其成为 L2TP 客户端。

1. 配置 L2TP 拨号连接：
   1） 进入 Windows XP 的“ 开始 ”→“ 设置 ”→“ 控制面板 ”，选择“ 切换到分类视图 ”。
   2） 选择“ 网络和 Internet 连接 ”。
   3） 选择“ 创建一个到您的工作位置的网络连接 ”。
   4） 选择“ 虚拟专用网络连接（V）”，单击“ 下一步 ”。
   5） 为连接输入一个名字为“ l2tp ”，单击“ 下一步 ”。
   6） 选择“ 不拨初始连接 ”，单击“ 下一步 ”。
   7） 输入准备连接的 L2TP 服务器的 IP 地址“ 202.101.35.218 ”，单击“ 下一步 ”。
   8） 单击“ 完成 ”。
   9） 双击“ l2tp ”连接，在 l2tp 连接窗口，单击“ 属性 ”。
   10） 选择“ 安全 ”属性页面，选择“ 高级（自定义设置）”，单击“ 设置 ”。
   11） 在“ 数据加密 ”中选择“ 可选加密（没有加密也可以连接）”。
   12） 在“ 允许这些协议 ”选中“ 不加密的密码（PAP）”、“ 质询握手身份验证协议（CHAP）”、“ Microsoft CHAP（MS-CHAP）”，单击“ 确定 ”。
   13） 选择“ 网络 ”属性页面，在“ VPN 类型 ”选择“ L2TP IPSec VPN ”。
   14） 确认“ Internet 协议（TCP/IP）”被选中。
   15） 确认“ NWLink IPX/SPX/NetBIOS Compatible Transport Prococol ”、“ 微软网络文件和打印共享 ”、“ 微软网络客户 ”协议没有被选中。
   16） 单击“ 确定 ”，保存所做的修改。

2. 修改注册表

缺省的 Windows XP L2TP 传输策略不允许 L2TP 传输不使用 IPSec 加密。可以通过修改 Windows XP 注册表来禁用缺省的行为：

方法一：在“ PPTP/L2TP 信息列表 ”中，单击“ 导出 WINDOWS 注册表文件 ”超链接，导出并运行 l2tp.reg 文件即可修改注册表，改动后重启电脑以使改动生效。

方法二：运行光盘\registry\目录下的 l2tp.reg 文件。

方法三：手工修改：
   1） 进入 Windows XP 的“ 开始 ”→“ 运行 ”里面输入“ Regedt32 ”，打开“ 注册表编辑器 ”，定位“ HKEY_Local_Machine \ System \ CurrentControl Set \ Services \ RasMan \ Parameters ”主键。
   2） 为该主键添加以下键值：
      键值：ProhibitIpSec
      数据类型：reg_dword
      值：1

3）保存所做的修改，重新启动电脑以使改动生效。

提示：必须添加“ ProhibitIpSec ”注册表键值到每个要使用 L2TP 的运行 Windows XP 操作系统的电脑。

3. 使用 L2TP 隧道连接到 HiPER L2TP 服务器
   1） 确认计算机已经连接到 Internet（可能是拨号连接或者是固定 IP 接入）。
   2） 启动前面步骤中创建的“ l2tp ”拨号连接。
   3） 输入 l2tp 连接的用户名“ vpn_mobile ”和密码“ vpntest ”。
   4） 单击“ 连接 ”。
   5） 连接成功后，在 MS-DOS 方式下输入“ ipconfig ”，可以看到一个在 HiPER L2TP 服务器地址池中的地址，就是 HiPER L2TP 服务器分配给本机的 IP 地址。

5.2.1.5 相关状态信息

在 ***VPN 配置—>PPTP 和 L2TP*** 中，可以查看“ PPTP/L2TP 信息列表 ”，检查 HiPER（作为 L2TP 服务器）连接以后的相关状态信息，如表 5-6、表 5-7 所示。

PPTP/L2TP 信息列表 2/16

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

	设置名	用户名	允许	会话状态	远端网关	远端内网地址	使用时间
☐	vpn_bj	vpn_bj	☑	已连接	202.101.35.217	192.168.16.1	00:00:09:1
☐	vpn_mobile	vpn_mobile	☑	已连接	192.168.123.10	192.168.210.34	00:00:00:0

表 5-6 HiPER 作为 L2TP 服务器 — PPTP-L2TP 信息列表

PPTP/L2TP 信息列表 2/128

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

	使用时间	空闲时间	出流量	入流量	业务类型	协议类型	虚接口地址	是否加密
	00:00:15:55	00:00:03:53	65074	60979	VPN拨入	L2TP	10.10.10.14	否
	00:00:02:28	00:00:00:01	12254	16776	VPN拨入	L2TP	10.10.10.15	否

表 5-7 HiPER 作为 L2TP 服务器 — VPN 信息列表（续表 5-6）

当 L2TP 客户端成功连接到 L2TP 服务器之后，“ 会话状态 ”由“ 关闭 ”变成“ 已连接 ”，“ 协议类型 ”显示为“ L2TP ”。同时“ 虚接口地址 ”显示为分配给 L2TP 客户端的 IP 地址。此时“ 使用时间 ”开始计时，如果隧道有数据流量，那么“ 出流量 ”和“ 入流量 ”则开始计数。如果隧道没有数据流量，那么“ 空闲时间 ”开始计时。

5.2.2 配置 HiPER 作为 L2TP 客户端

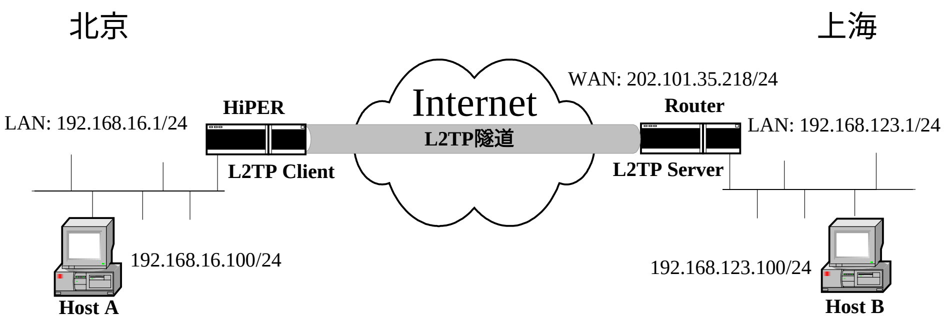


图 5-6 方案——HiPER 作为 L2TP 客户端

在本方案中，某公司总部在上海。在北京有一个分公司希望可以实现两地局域网内部资源的相互访问。

本方案使用 L2TP 协议建立 VPN 隧道，如图 5-6 所示，在上海公司总部使用任意品牌的标准 VPN 路由器(推荐使用 HiPER VPN 网关)作为 L2TP 服务器,在北京使用 HiPER VPN 网关作为 L2TP 客户端。地址如下：

北京（L2TP 客户端）：

局域网网段 IP 地址：192.168.16.0/255.255.255.0

HiPER 的 LAN 口 IP 地址：192.168.16.1/255.255.255.0

上海（L2TP 服务器）：

局域网网段 IP 地址：192.168.123.0/255.255.255.0

路由器的 LAN 口 IP 地址：192.168.123.1/255.255.255.0

路由器的 WAN 口 IP 地址：202.101.35.218/255.255.255.0

5.2.2.1 配置 HiPER 作为 L2TP 客户端（LAN 到 LAN）

在 ***VPN 配置—>PPTP 和 L2TP*** 中，选择 " 添加 " 选项，然后在配置参数项中依次输入以下内容，再单击 " 保存 " 按钮。

" 设置名 "：vpn_sh

" 业务类型 "：拨出（客户端）

" 用户名 "：vpn_bj

" 协议类型 "：L2TP

" 密码 "：vpntest

" 确认密码 "：vpntest

" 密码验证方式 "：PAP

" 远端内网 IP 地址 "：192.168.123.1（VPN 隧道对端局域网所使用的 IP 地址）

" 远端内网子网掩码 "：255.255.255.0

" 隧道服务器地址(名) "：202.101.35.218

5.2.2.2 配置 HiPER 作为 L2TP 服务器（LAN 到 LAN）

配置同章节 5.2.1.1（配置 HiPER 作为 L2TP 服务器）。

5.2.2.3 配置 Windows 2000 Server 作为 L2TP 服务器（LAN 到 LAN）

按照以下步骤配置 Windows 2000 Server 计算机，使其成为 PPTP 服务器。

1. 配置 " 路由和远程访问 " 服务：
   1） 进入 Windows 2000 Server 的 " 开始 " → " 程序 " → " 管理工具 " → " 路由和远程访问 " 配置界面，如图 5-7 所示。

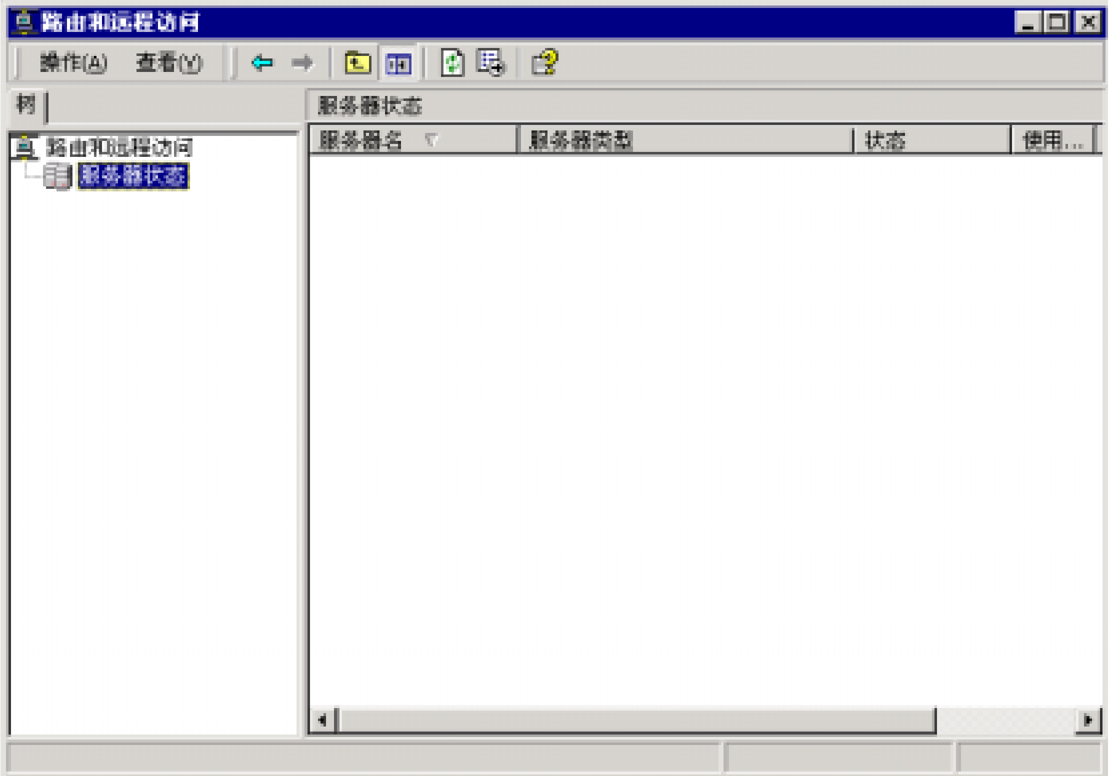


图 5-7 路由和远程访问界面一

2） 选择 " 服务器状态 "，单击鼠标右键，选择 " 添加服务器 "。

3） 选择 " 这台计算机 "，单击 " 确定 "，出现如图 5-8 所示界面。

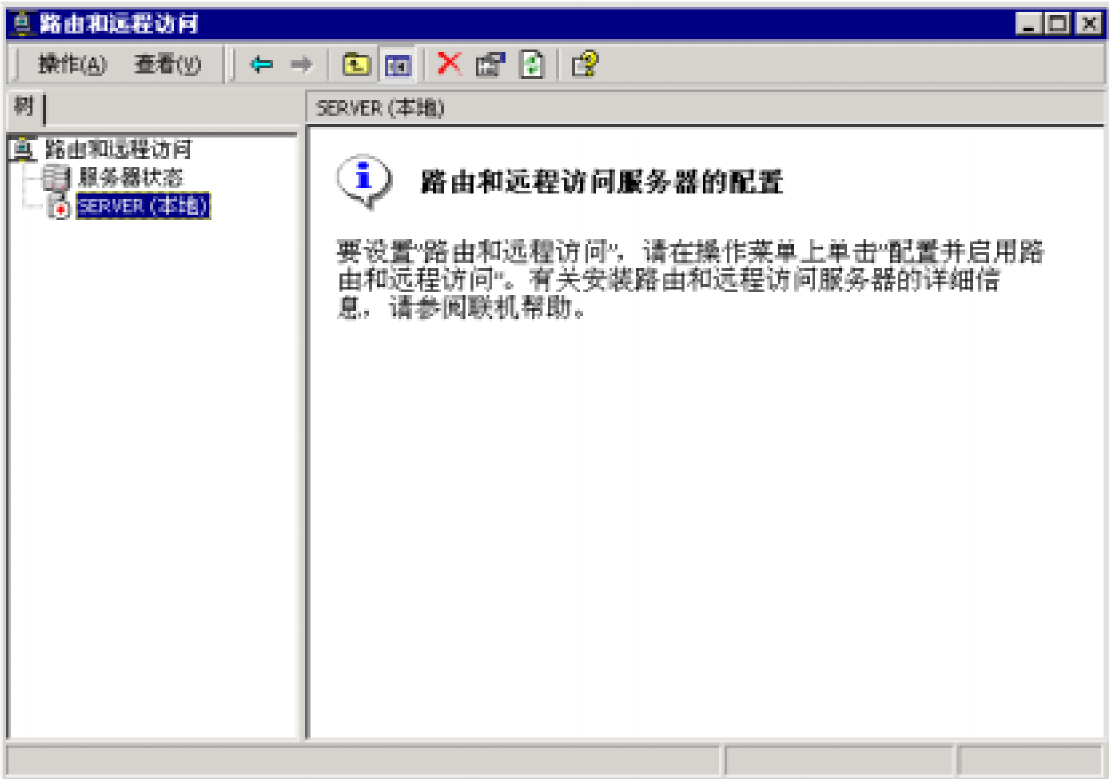


图 5-8 路由和远程访问界面二

4） 选择上一步添加的计算机，单击鼠标右键，选择 " 配置和启用路由和远程访问 "。

5） 单击 “ 下一步 ”。
6） 选择 “ 手动配置服务器 ”，单击 “ 下一步 ”。
7） 单击 “ 完成 ”。
8） 单击 “ 是 ”，以开启 “ 路由和远程访问 ” 服务，如图 5-9 所示。

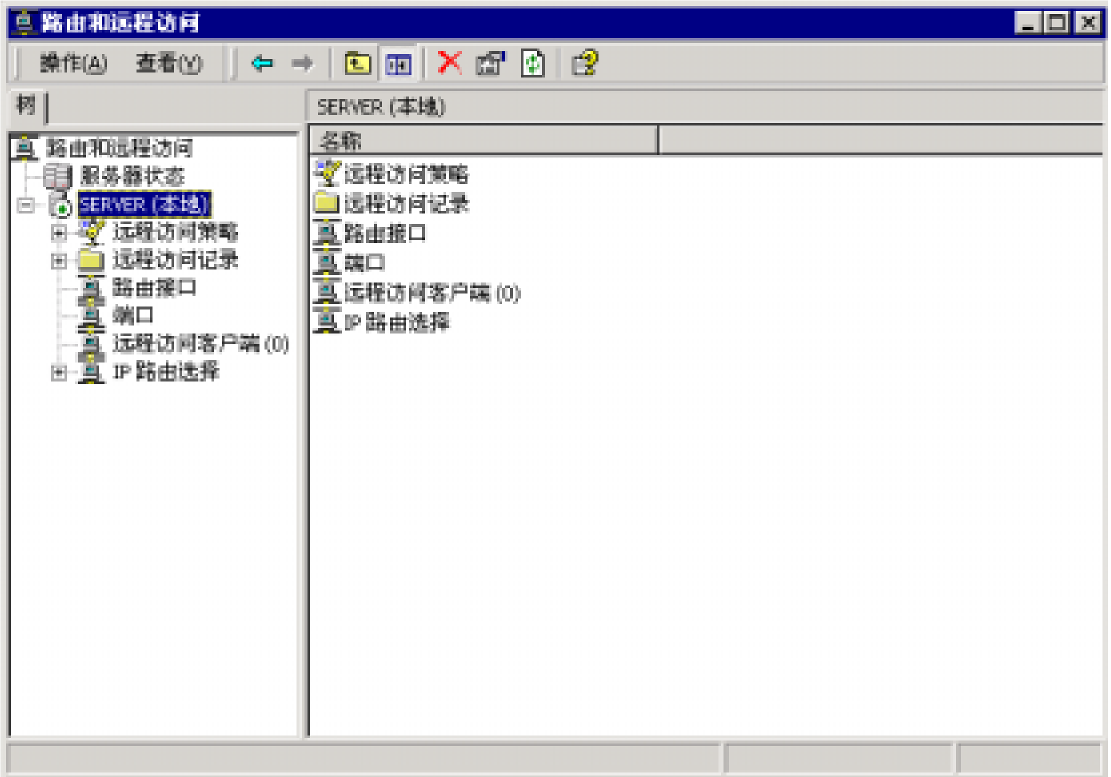


图 5-9 路由和远程访问界面三

9） 选择 “ SERVER ”，单击鼠标右键，选择 “ 属性 ”。

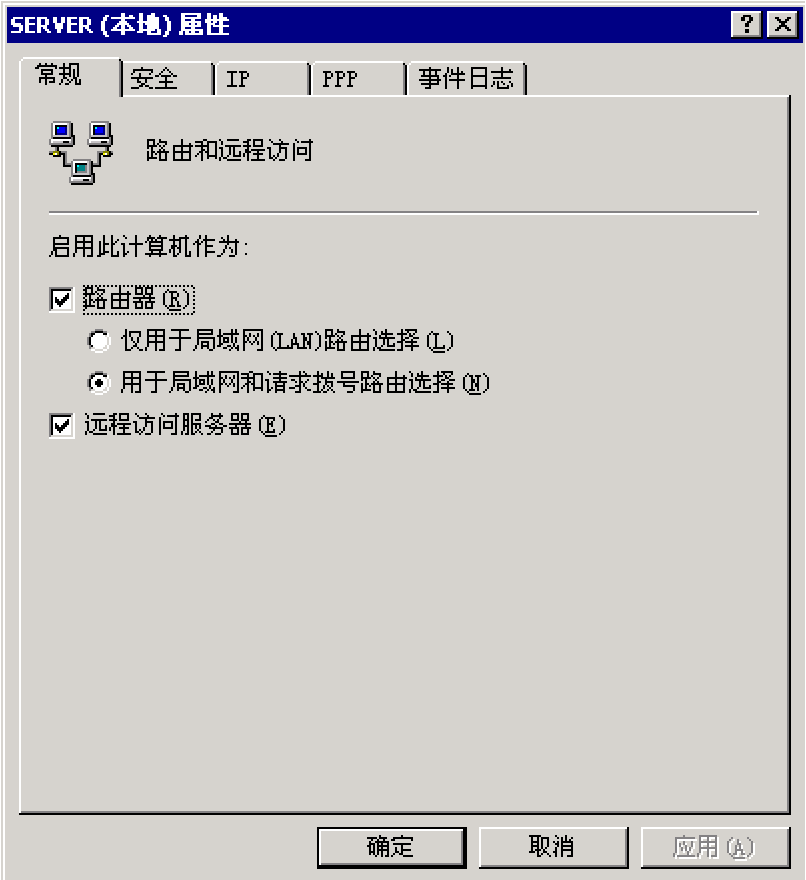


图 5-10 SERVER（本地）属性界面

10）进入“常规”属性页面，在“启用此计算机作为”选中“路由器”、“用于局域网和请求拨号路由选择”、“远程访问服务器”，如图 5-10 所示。

11）进入“安全”属性页面，在“验证提供程序”，选择“Windows 身份验证”，单击“身份验证方法”。

12）选中“Microsoft 加密身份验证（MS-CHAP）”、“加密身份验证（CHAP）”、“不加密的密码（PAP）”，单击“确定”，如图 5-11 所示。

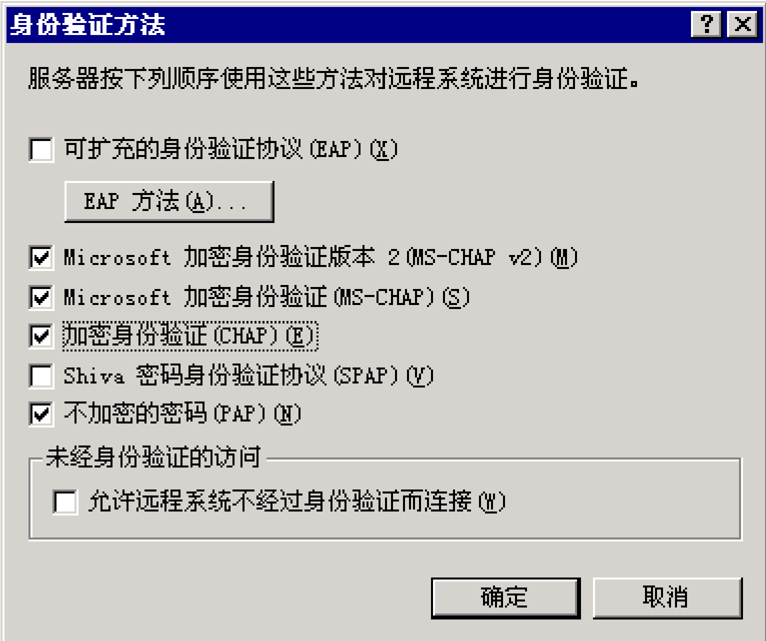


图 5-11 身份验证方法界面

13）进入“IP”属性页面，选中“启用 IP 路由”，选中“允许基于 IP 的远程访问和请求拨号连接”。选择“静态地址池”，单击“添加”。

14）输入起始 IP 地址“192.168.123.201”，地址数“50”（输入 Windows 2000 Server 局域网端口所在网段一段空闲的 IP 地址），单击“确定”，如图 5-12 所示。

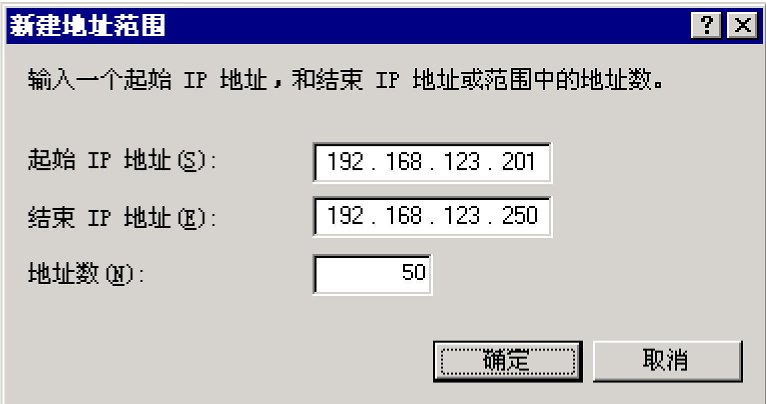


图 5-12 新建地址范围界面

15）在“适配器”，选中“允许 RAS 选择适配器”（如果计算机只安装了一块网卡，看不到此选项），单击“确定”。

16）选择“远程访问策略”，单击鼠标右键，选择“新建远程访问策略”。

17）填入远程访问策略的名称“vpn”，单击“下一步”。

18）单击“添加”。

19）选中“NAS-Port-Type”，单击“添加”。

20）将“可用类型”“Virtual（VPN）”添加到“选择的类型”中，单击“确定”，如图 5-13 所示。

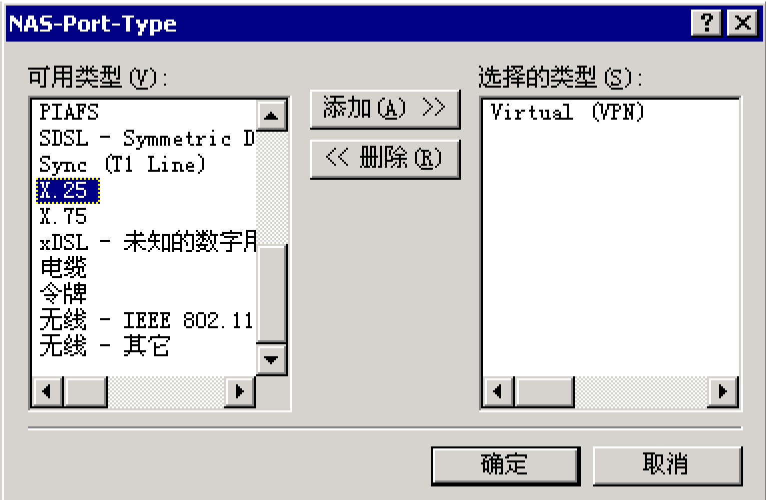


图 5-13 NAS-Port-Type 界面

21）单击“下一步”。

22）选中“授予远程访问权限”，单击“下一步”。

23）单击“编辑配置文件”。

24）在“身份验证”属性页面，选中“Microsoft 加密身份验证（MS-CHAP）”、“加密身份验证（CHAP）”、“未加密的密码（PAP，SPAP）”，单击“确定”，如图 5-14 所示。

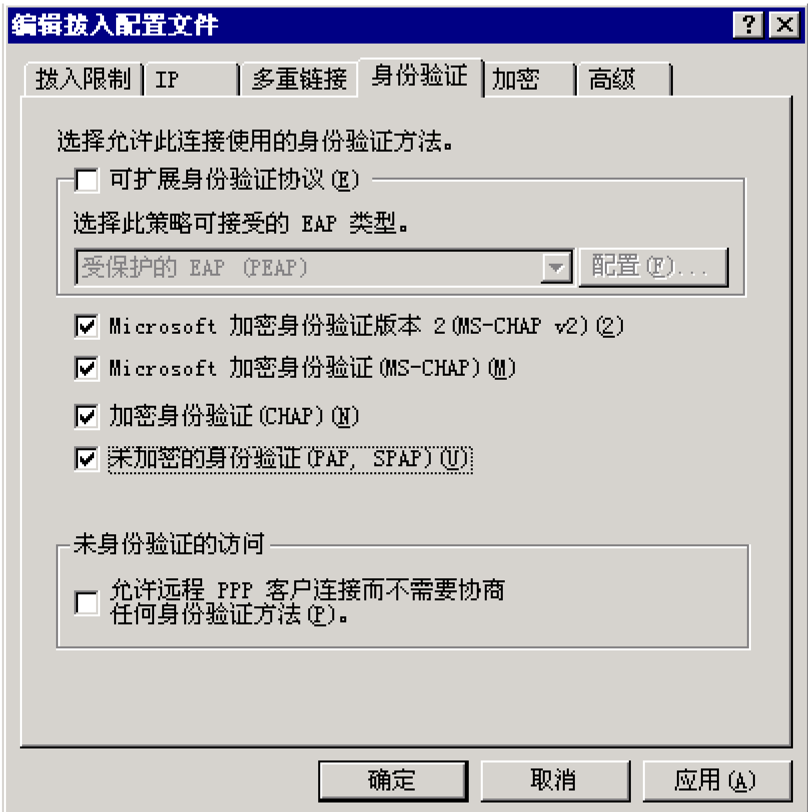


图 5-14 编辑拨入配置文件界面

25）单击“确定”。

26）选中“端口”，单击鼠标右键，选择“属性”。

27）选中“ WAN 微型端口（L2TP）”，单击“ 配置 ”。

28）根据实际 L2TP 客户端的数量，调整“ 最多端口数 ”，单击“ 确定 ”，如图 5-15 所示。

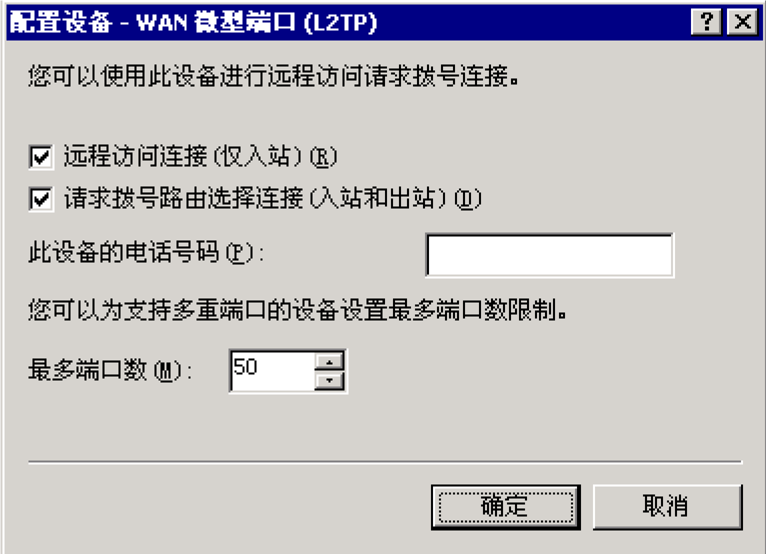


图 5-15 配置设备界面

29）路由和远程访问服务配置完成。

3. 修改注册表 缺省的 Windows 2000 Server 传输策略不允许 L2TP 传输不使用 IPSec 加密。可以通过修改 Windows 2000 Server 注册表来禁用缺省的行为。

方法一：运行光盘\registry\目录下的 l2tp.reg 文件。

方法二：手工修改：

1） 进入 Windows 2000 的“ 开始 ”→“ 运行 ”里面输入“ Regedt32 ”，打开“ 注册表编辑器 ”, 定位“ HKEY_Local_Machine \ System \ CurrentControl Set \ Services \ RasMan \ Parameters ”主键。

2） 选择编辑→添加数值，为该主键添加以下键值：

数值名称：ProhibitIpSec

数据类型：reg_dword

值：1

3） 保存所做的修改，重新启动电脑以使改动生效。

4. 配置拨入的 L2TP 用户帐号：

1） 进入 Windows 2000 Server 的“ 开始 ”→“ 程序 ”→“ 管理工具 ”→“ 计算机管理 ”（注意：如果配置了 Windows 2000 Server 成为域控制器，可以在 Active Directory 的用户管理中添加用户帐号）。

2） 选中“ 本地用户和组 ”→“ 用户 ”，单击鼠标右键，选择“ 新用户 ”，进入如图 5-16 所示界面。

3） 首先依次填入以下参数：

“ 用户名 ”：vpn_bj

“ 密码 ”：vpntest

“ 确认密码 ”：vpntest

“ 用户下次登录时须更改密码 ”：取消选中

“ 用户不能更改密码 ”：选中

"密码永不过期"：选中
然后单击"创建"。

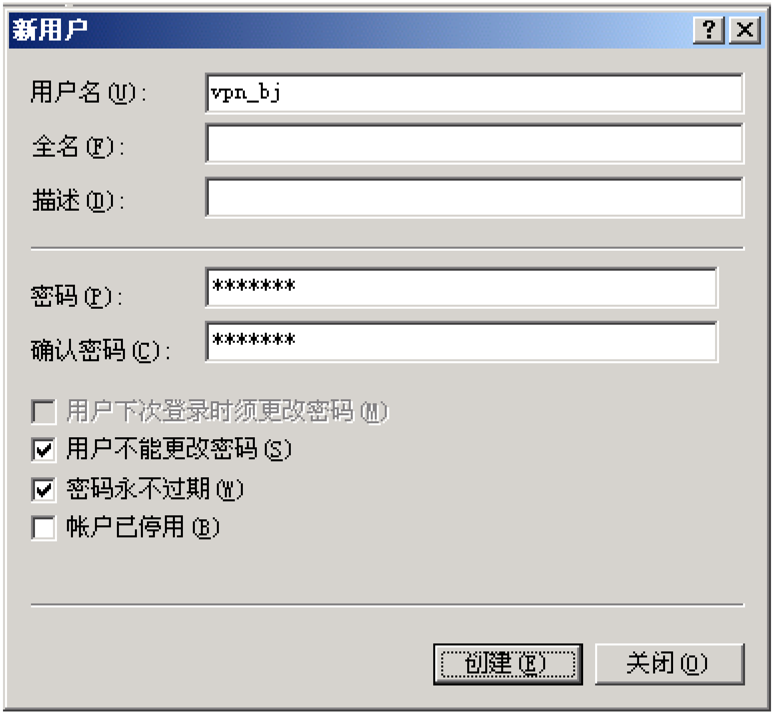


图 5-16 新用户界面

4) 选中上一步新建的"vpn_bj"用户，单击鼠标右键，选择"属性"。
5) 在"拨入"属性页面，在"远程访问权限"选择"通过远程访问策略控制访问"。
6) 在"回拨选项"选择"不回拨"。
7) 选中"分配静态 IP 地址"，从地址池中选择一个 IP 地址 192.168.123.240（在"路由和远程访问"中第 14 步配置）作为分配给此帐号的 IP 地址。
8) 选中"应用静态路由"。
9) 单击"添加路由"，进入如图 5-17 所示界面。
10) 填入北京路由器局域网的网段，目标：192.168.16.0，网络掩码：255.255.255.0，跃点数"1"，单击"确定"。

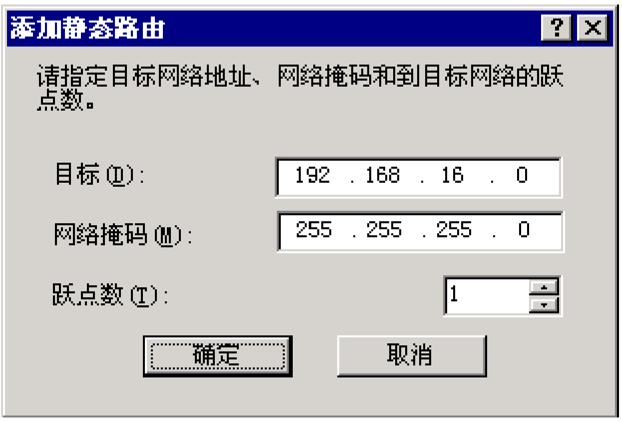


图 5-17 添加静态路由界面

11) 单击两次"确定"。
12) L2TP 用户帐号配置完成。

5. 查看 L2TP 隧道连接状态：

进入 Windows 2000 Server 的“开始”→“程序”→“管理工具”→“路由和远程访问”，选中“远程访问客户端”，可以在窗口右侧看到拨入的用户信息。

双击拨入的用户，可以查看一些实时的 L2TP 隧道连接状态信息，如图 5-18 所示。

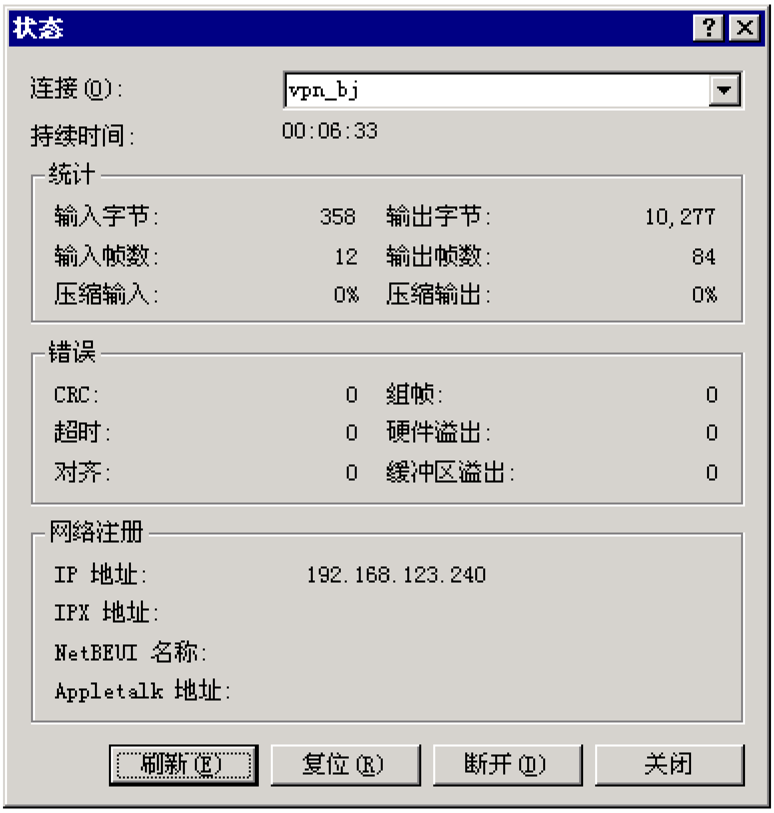


图 5-18 VPN 状态信息界面

5.2.2.4 配置 Cisco 路由器作为 L2TP 服务器（LAN 到 LAN）

按照以下步骤配置 Cisco 路由器，使其成为 L2TP 服务器。Cisco 在做 VPN 接入的时候，必须配置 Radius Server 为 Cisco 验证用户身份、添加用户路由。

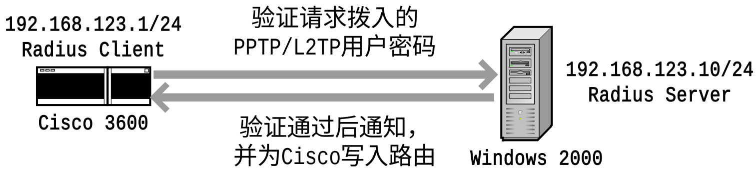


图 5-19 方案——Cisco 路由器作为 L2TP 服务器

1. 配置 Cisco 成为 L2TP 服务器

//配置 L2TP 服务器的全局参数

vpdn enable

vpdn-group 1

accept-dialin

protocol L2TP

virtual-template 1

local name runway
lcp renegotiation always
no l2tp tunnel authentication

//配置 L2TP 服务器的 Virtual-Template（IP 地址 unnumbered 路由器 WAN 口）

interface Virtual-Template1
ip unnumbered Ethernet0/0
peer default ip address pool default
ppp authentication pap

//配置 L2TP 地址池

ip local pool default 10.0.0.1 10.0.0.254

2. 配置 Cisco 的成为 Radius client

//配置一个 Cisco 访问帐号

username admin password admin321

//配置 Cisco 的 AAA

aaa new-model
aaa authentication login default local
aaa authentication ppp default group radius local
aaa authorization network default group radius local
aaa accounting exec default start-stop group radius
aaa accounting network default start-stop group radius

//配置 Radius Server 的 IP 地址和口令

radius-server host 192.168.123.10 auth-port 1812 acct-port 1813
radius-server retransmit 3
radius-server key testing123

3. 在 Windows 2000 Server 上安装“ Internet 验证服务 ”：
   1） 进入 Windows 2000 Server 的“ 开始 ”→“ 设置 ”→“ 控制面板 ”→“ 添加/删除程序 ”。
   2） 选择“ 添加/删除 Windows 组件 ”。
   3） 选择组件→网络服务→ Internet 验证服务，单击确定。
   4） 如果需要的话插入 Microsoft Windows 2000 Server 安装软盘或者 CD。

4. 配置 Windows2000 Serve 的“ Internet 验证服务 ”：
   1） 进入 Windows 2000 Server 的“ 开始 ”→“ 程序 ”→“ 管理工具 ”→ “ Internet 验证服务 ”配置界面，如图 5-20 所示。

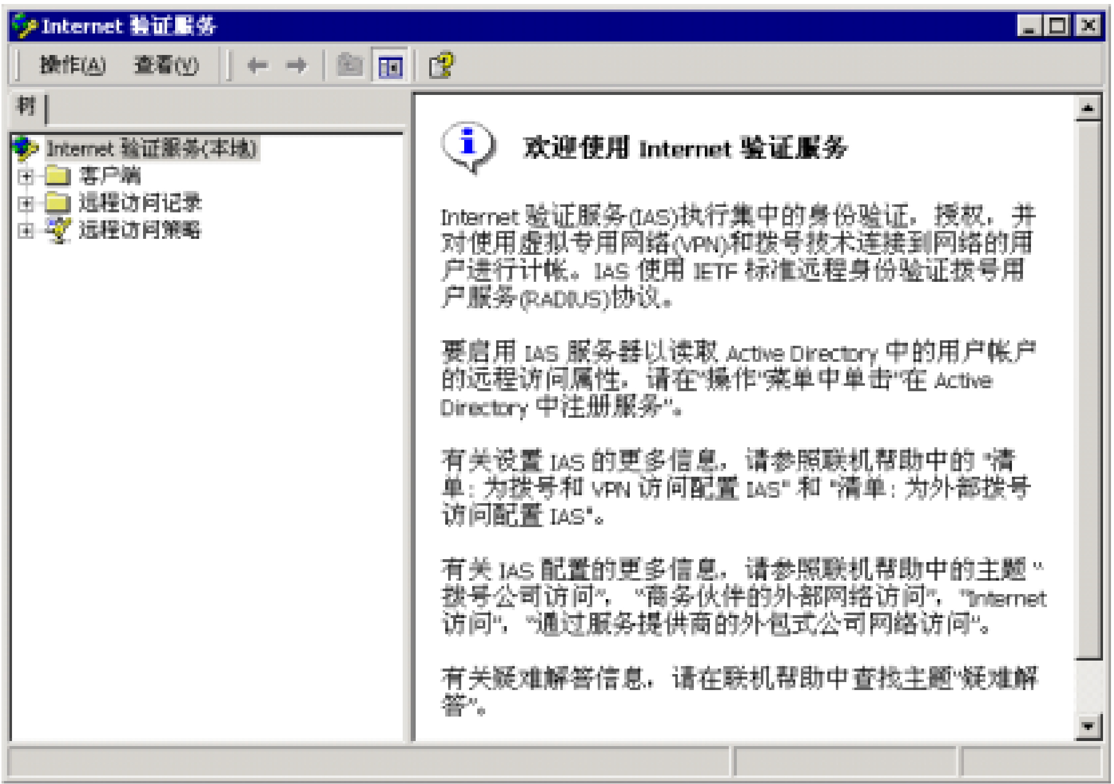


图 5-20 Internet 验证服务界面

2） 选中“客户端”，单击鼠标右键，选择“新建客户端”。
3） “为客户端输入一个好记的名称”填入“cisco”，“协议”选择“RADIUS”，单击下一步。
4） 填入“客户端地址（IP 或 DNS）”：192.168.123.1；“客户端-供应商”：RADIUS Standard；“共享的机密”：testing123；“确认共享的机密”：testing123。确认“客户端必须总是在请求中发送签名属性”没有被选中，然后单击“完成”，如图 5-21 所示。

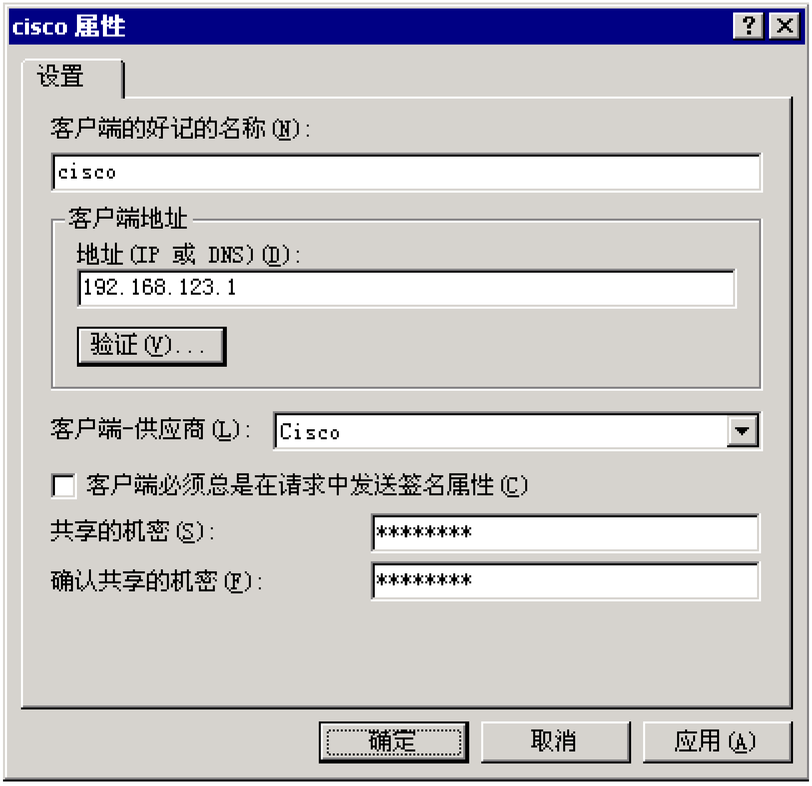


图 5-21 cisco 属性界面

5） 选择“ 远程访问策略 ”，单击鼠标右键，选择“ 新建远程访问策略 ”。

6） 填入远程访问策略的名称“ cisco ”，单击“ 下一步 ”。

7） 单击“ 添加 ”，进入如图 5-22 所示界面。

8） 选中“ Day-And-Time-Restrictions ”，单击“ 添加 ”，进入如图 5-23 所示界面。

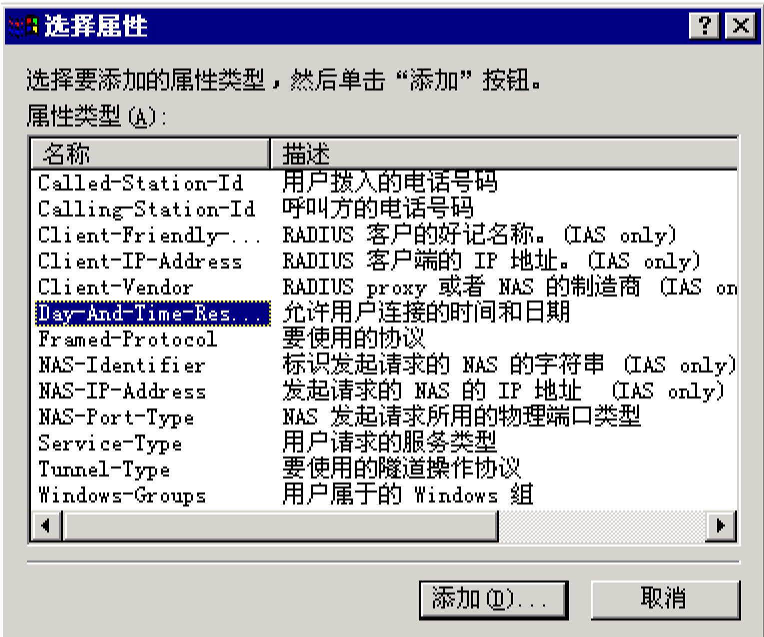


图 5-22 选择属性界面

9） 选择“ 允许 ”，单击确定。

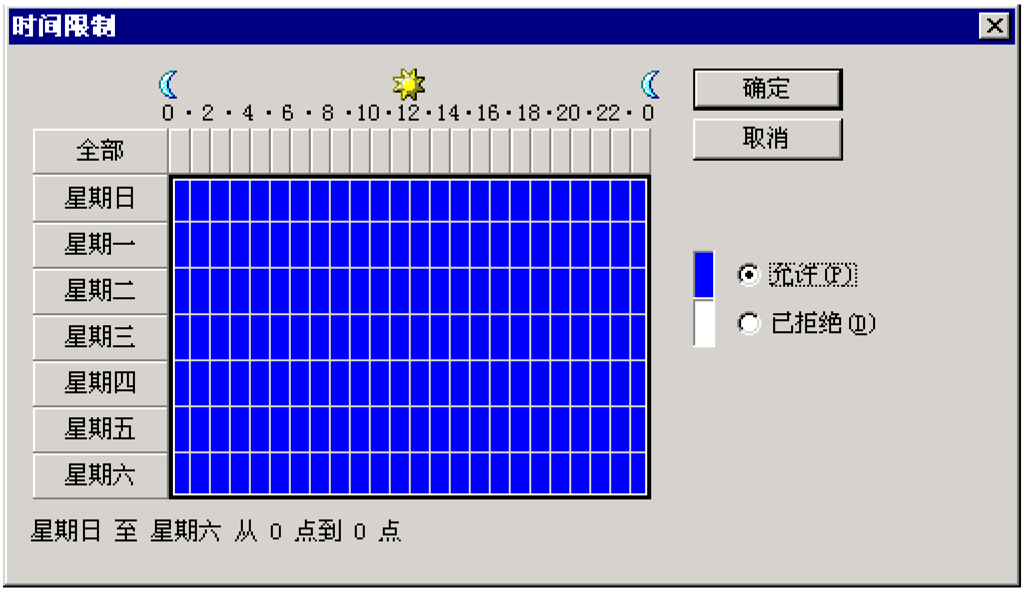


图 5-23 时间限制界面

10）选中“授予远程访问权限”，单击“下一步”。

11）单击“编辑配置文件”。

12）在“身份验证”属性页面（如图 5-24 所示），选中“Microsoft 加密身份验证（MS-CHAP）”、“加密身份验证（CHAP）”、“未加密的密码（PAP，SPAP）”，单击确定。

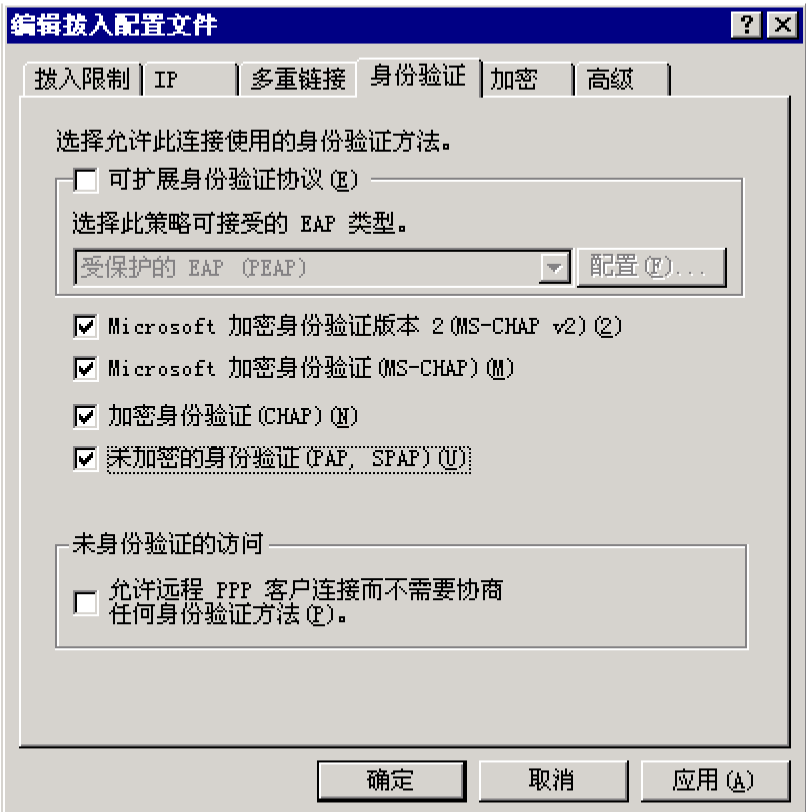


图 5-24 时间限制界面

13）单击“确定”。

5. 配置拨入的 L2TP 用户帐号：

1） 进入 Windows 2000 Server 的“开始”→“程序”→“管理工具”→“计算机管理”（注意：如果配置了 Windows 2000 Server 成为域控制器，可以在 Active Directory 的用户管理中添加用户帐号）。
2） 选中“本地用户和组”→“用户”，单击鼠标右键，选择“新用户”，进入如图 5-25 所示界面。
3） 首先依次填入以下参数：
“用户名”：vpn_bj
“密码”：vpntest
“确认密码”：vpntest
“用户下次登录时须更改密码”：取消选中
“用户不能更改密码”：选中
“密码永不过期”：选中
然后单击“创建”。

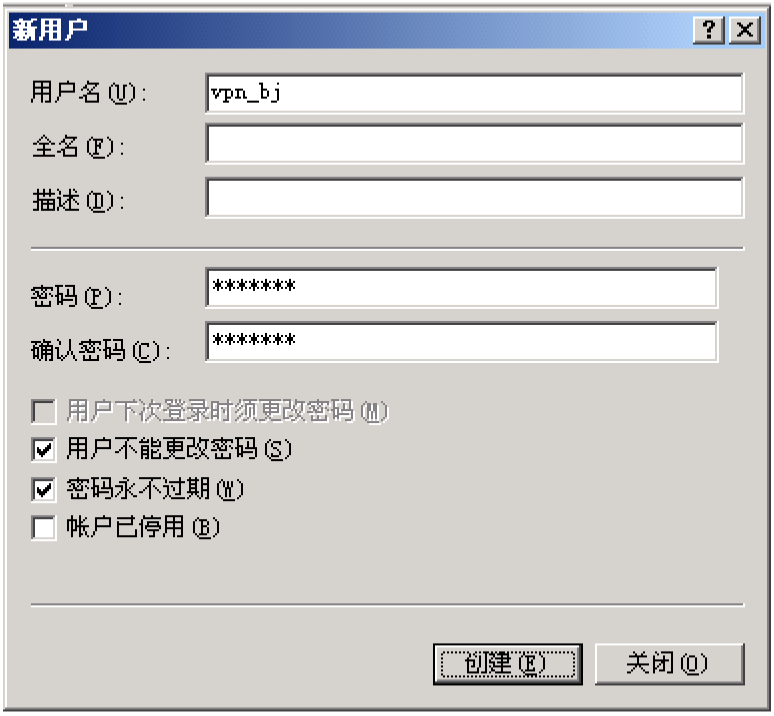


图 5-25 新用户界面

4） 选中上一步新建的“vpn_bj”用户，单击鼠标右键，选择“属性”。
5） 在“拨入”属性页面，在“远程访问权限”选择“通过远程访问策略控制访问”。
6） 在“回拨选项”选择“不回拨”。
7） 选中“分配静态 IP 地址”，从 Cisco VPN 地址池中选择一个 IP 地址 10.0.0.123（在“路由和远程访问”中第 14 步配置）作为分配给此帐号的 IP 地址。
8） 选中“应用静态路由”。
9） 单击“添加路由”，进入如图 5-26 所示界面。
10） 填入北京路由器局域网的网段，目标：192.168.16.0，网络掩码：255.255.255.0，跃点数“1”，单击确定。

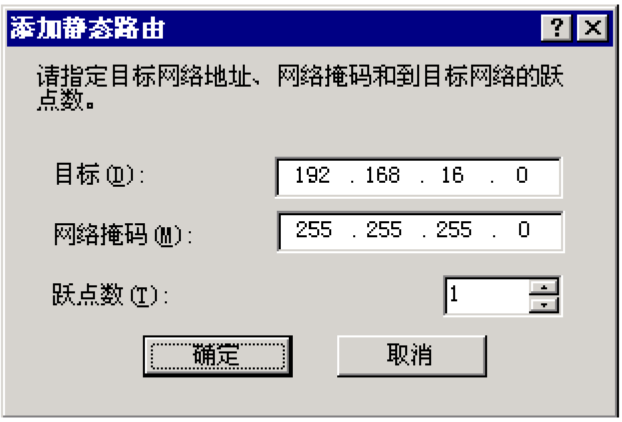


图 5-26 添加静态路由界面

11） 单击两次“ 确定 “ 。

12） VPN 用户帐号配置完成。

5.2.2.5 配置 Fortigate 防火墙作为 L2TP 服务器（LAN 到 LAN）

按照以下步骤配置 Fortigate 防火墙，使其成为 L2TP 服务器。

1. 配置用户：

1） 进入的 Fortigate 防火墙“ 设置用户 ”→“ 本地 ”页面，单击“ 新建 ”，进入如图 5-27 所示界面。

2） 输入 L2TP VPN 的“ 用户名称 ”为“ vpn_bj ”;“ 输入密码 ”为“ vpntest ”，单击确定

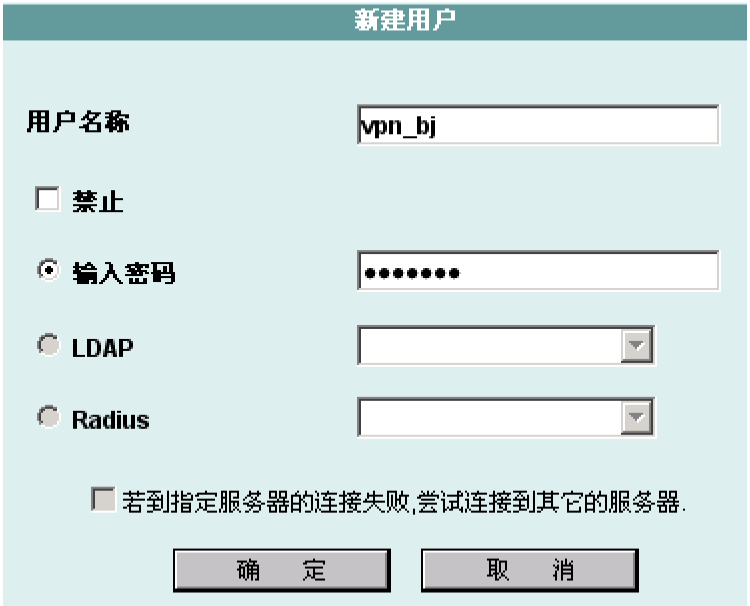


图 5-27 新建用户界面

2. 配置用户组：

1） 进入 Fortigate 防火墙的“ 设置用户 ”→“ 用户组 ”，单击“ 新建 ”，进入如图 5-28 所示界面。

2） 填入“ 组名 ”为“ l2tp ”，将“ vpn_bj ”用户添加到组员中去。单击“ 确定 ”。

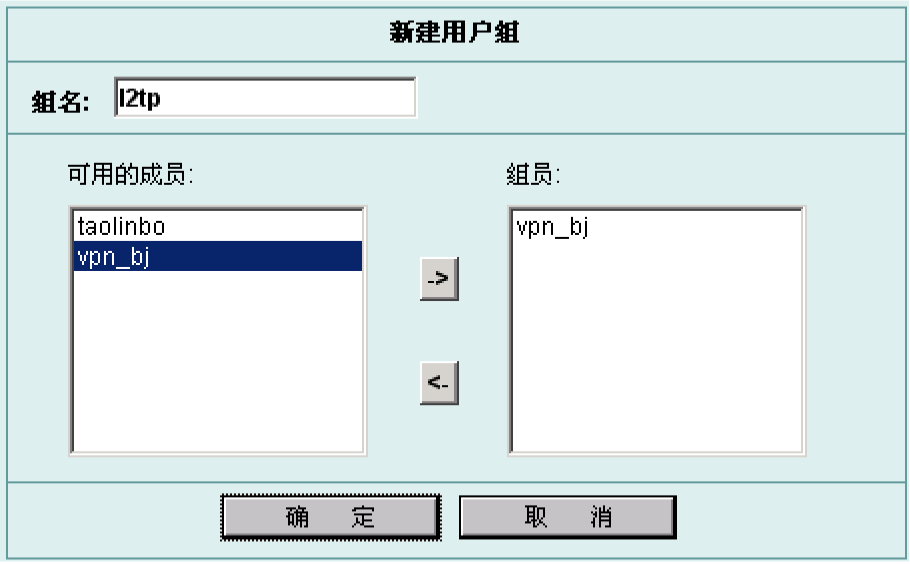


图 5-28 新建用户组界面

3. 启用 L2TP：
   1）进入 Fortigate 防火墙的“虚拟专网”→“L2TP”，进入如图 5-29 所示界面。
   2）选中“启用 L2TP”，设置“起始 IP”为 192.168.18.210，“终止 IP”为 192.168.18.220（任意其他网段一段空闲的 IP 地址），“用户组”选择上一步新建的“l2tp”用户组，单击提交。

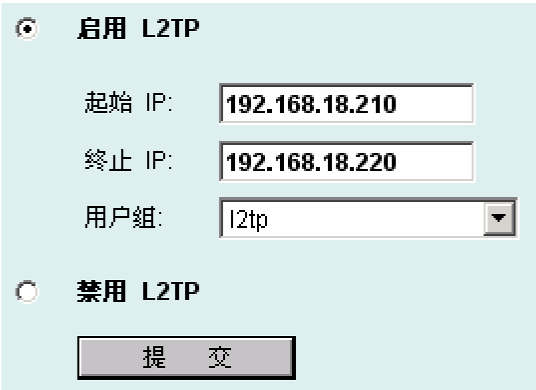


图 5-29 启用 L2TP 界面

4. 设置防火墙策略：
   1）进入 Fortigate 防火墙的“防火墙”→“地址”页面。
   2）选择“外部接口”为“internal”，单击“新建”，进入如图 5-30 所示界面。
   3）设置地址名称为“lan123”，“IP 地址”、“子网掩码”为 Fortigate 防火墙的局域网网段“192.168.123.0”、“255.255.255.0”，单击“确定”。

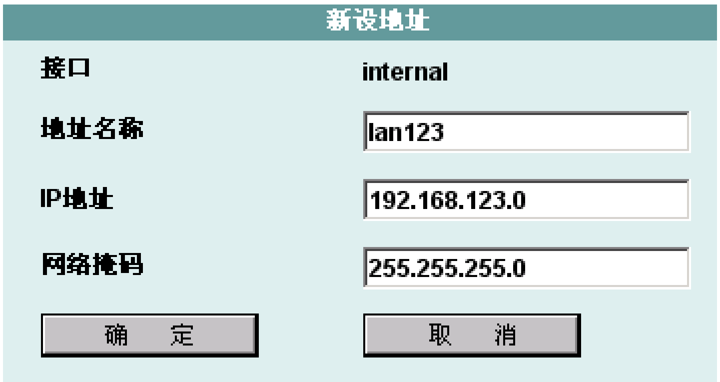


图 5-30 新设地址界面一

4) 选择“外部接口”为“wan1”（Fortigate 防火墙的 Internet 接口），单击“新建”，进入如图 5-31 所示界面。
5) 设置地址名称为“vpn18”，“IP 地址”、“子网掩码”为第 3 步设置的 Fortigate 防火墙的 L2TP 地址池所在的网段“192.168.18.0”、“255.255.255.0”，单击确定。

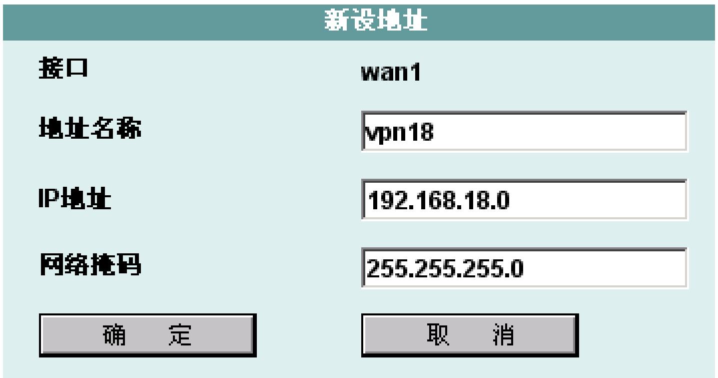


图 5-31 新设地址界面二

6) 进入 Fortigate 防火墙的“防火墙”→“策略”页面。
7) 单击“wan1→ internal”接口，进入“wan1→ internal”策略设置界面，单击新建，进入如图 5-32 所示界面。
8) “来源”地址选择上面设定的‘vpn18’地址段，“目的”地址选择上面设定的‘lan123”地址段，完成其他防火墙设置策略后单击确定。



图 5-32 新建输出策略界面

提示：Fortigate 防火墙只支持移动用户的接入，如果想实现一个局域网通过路由器连接到 Fortigate 防火墙，就必须在 PPTP/L2TP 隧道上启用 NAT，可以参考章节 2.4.1 里面的设置，但是这样只能是实现 PPTP/L2TP 客户端局域网到

Fortigate 防火墙端局域网的单向访问。

5.2.2.6 相关状态信息

在 ***VPN 配置—>PPTP 和 L2TP*** 的“ PPTP/L2TP 信息列表 ”中，检查 HiPER VPN 网关（作为 L2TP 客户端）连接前后的相关状态信息，如表 5-8、表 5-9 所示：

PPTP/L2TP 信息列表 1/129

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

	设置名	用户名	允许	会话状态	远端网关	远端内网地址	使用时间
☐	vpn_sh	vpn_bj	☑	已连接	202.101.35.218	192.168.123.1	00:00:04:20

表 5-8 HiPER 作为 L2TP 客户端 — PPTP/L2TP 信息列表

PPTP/L2TP 信息列表 1/129

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

使用时间	空闲时间	出流量	入流量	业务类型	协议类型	虚接口地址	是否加密
0:00:04:20	00:00:04:20	4875	4898	VPN拨出	L2TP	10.10.10.10	否

表 5-9 HiPER 作为 L2TP 客户端 — PPTP/L2TP 信息列表（续表 5-8）

当 L2TP 客户端成功连接到 L2TP 服务器之后，“ 会话状态 ”由“ 关闭 ”变成“ 已连接 ”，同时获得 L2TP 服务器分配的“ 虚接口地址 ”为“ 10.10.10.10 ”。此时“ 使用时间 ”开始计时，如果隧道有数据流量，那么“ 出流量 ”和“ 入流量 ”则开始计数。如果隧道没有数据流量，那么“ 空闲时间 ”开始计时。

5.3 PPTP 配置实例

5.3.1 配置 HiPER 作为 PPTP 服务器

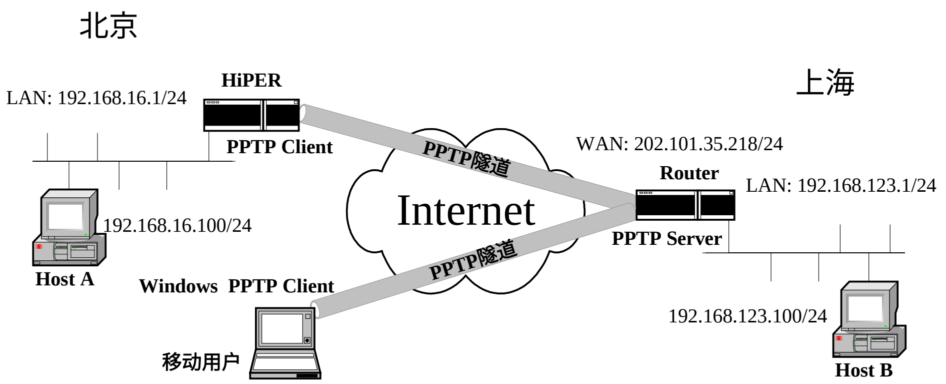


图 5-33 方案——HiPER 作为 PPTP 服务器

在本方案中，某公司总部在上海。在北京有一个分公司希望可以实现两地局域网内部资源的相互访问。该公司还有一些出差和远程办公的移动用户希望在远程访问总公司局域网内部资源。

本方案使用 PPTP 协议建立 VPN 隧道，在上海公司总部使用 HiPER VPN 网关作为 PPTP

服务器，在北京放置任意品牌的标准 VPN 路由器（推荐使用 HiPER VPN 网关）作为 PPTP 客户端，移动用户使用 Windows 操作系统内置的 PPTP 客户端软件。地址如下：

上海（PPTP 服务器）：

局域网网段 IP 地址：192.168.123.0/24；

HiPER 的 LAN 口 IP 地址：192.168.123.1/24；

HiPER 的 WAN 口 IP 地址：202.101.35.218/24；

北京（PPTP 客户端）：

局域网网段 IP 地址：192.168.16.0/24；

路由器的 LAN 口 IP 地址：192.168.16.1/24；

移动用户（PPTP 客户端）：

使用 Windows 操作系统通过 PPTP 拨号建立 PPTP 隧道连接。

5.3.1.1 配置 HiPER 作为 PPTP 服务器（LAN 到 LAN /移动用户拨入）

1. 为北京的路由器创建 PPTP 隧道拨入帐号

在 ***VPN 配置—>PPTP 和 L2TP*** 中，选择“ 添加 ”选项，然后在配置参数项中依次输入以下内容：

“ 设置名 ”：vpn_bj

“ 业务类型 ”：拨入（服务器）

“ 用户类型 ”：LAN 到 LAN

“ 密码 ”：vpntest

“ 确认密码 ”：vpntest

“ 密码验证方式 ”：PAP

“ 远端内网 IP 地址 ”：192.168.16.1（VPN 隧道对端局域网所使用的 IP 地址）

“ 远端内网网络掩码 ”：255.255.255.0

“ 分配 IP 地址 ”：选中

“ 地址池开始地址 ”：10.10.10.10（不能和整个 VPN 方案中所有 IP 地址段重复）

“ 地址池地址数 ”：50

再单击“ 保存 ”按钮。

2. 为移动用户创建 PPTP 隧道拨入帐号

在 ***VPN 配置—>PPTP 和 L2TP*** 中，选择“ 添加 ”选项，然后在配置参数项中依次输入以下内容：

“ 设置名 ”：vpn_mobile

“ 业务类型 ”：拨入（服务器）

“ 用户类型 ”：移动用户

“ 密码 ”：vpntest

“ 确认密码 ”：vpntest

“ 密码验证方式 ”：PAP

“ 分配 IP 地址 ”：选中（同本节 1 中配置）

“ 地址池开始地址 ”：10.10.10.10（同本节 1 中配置）

“ 地址池地址数 ”：50（本节同 1 中配置）

再单击“ 保存 ”按钮。

5.3.1.2 配置 HiPER 作为 PPTP 客户端（LAN 到 LAN）

配置同章节 5.3.2.1（配置 HiPER 作为 PPTP 客户端）。

5.3.1.3 配置 Windows 2000 作为 PPTP 客户端（移动用户）

按照以下步骤配置 Windows 2000 计算机，使其成为 PPTP 客户端。

1. 配置 PPTP 拨号连接：
   1）进入 Windows 2000 的“开始”→“设置”→“网络和拨号连接”→“新建连接”。
   2）启动“网络连接向导”，单击“下一步”。
   3）在“网络连接类型”中，选择“通过 Internet 连接到专用网络”，单击“下一步”。
   4）选择“不拨初始连接”，单击“下一步”。
   5）在“目的地址”一栏，输入准备连接的 PPTP 服务器的 IP 地址“202.101.35.218”，单击“下一步”。
   6）选择“只是我自己使用此连接”，单击“下一步”。
   7）输入“您为这个连接使用的名称”为“pptp”。
   8）单击“完成”。
   9）双击“pptp”连接，在 pptp 连接窗口，单击“属性”。
   10）选择“安全措施”属性页面，选择“高级（自定义设置）”，单击“设置”。
   11）在“数据加密”中选择“可选加密（没有加密也可以连接）”。
   12）在“允许这些协议”选中“不加密的密码（PAP）”、“质询握手身份验证协议（CHAP）”、“Microsoft CHAP（MS-CHAP）”，单击“确定”。
   13）选择“网络”属性页面，在“我正在呼叫的 VPN 服务器的类型”选择“点对点隧道协议（PPTP）”。
   14）选择“网络”属性页面。
   15）确认“NWLink IPX/SPX/NetBIOS Compatible Transport Prococol”协议没有被选中。
   16）单击“确定“，保存所做的修改。

2. 使用 PPTP 隧道连接到 HiPER PPTP 服务器：
   1）确认计算机已经连接到 Internet（可能是拨号连接或者是固定 IP 接入）。
   2）启动前面步骤中创建的“pptp”拨号连接。
   3）输入的 PPTP 隧道的用户名“vpn_mobile”和密码“vpntest”。
   4）单击“连接“。
   5）连接成功后，在 MS-DOS 方式下输入“ipconfig”，可以看到一个在 PPTP 服务器地址池中的地址，就是 PPTP 服务器分配给本机的 IP 地址。

5.3.1.4 配置 Windows XP 作为 PPTP 客户端（移动用户）

按照以下步骤配置 Windows XP 计算机，使得它能够连接到 HiPER PPTP 服务器。

1. 配置 PPTP 拨号连接：
   1）进入 Windows XP 的“开始”→“设置”→“控制面板”，选择“切换到分类视图”。
   2）选择“网络和 Internet 连接”。
   3）选择“建立一个您的工作位置的网络连接”。
   4）选择“虚拟专用网络连接”，单击“下一步”。
   5）为连接输入一个名字为“pptp”，单击“下一步”。

6） 选择“ 不拨此初始连接 ”，单击“ 下一步 ”。
7） 输入准备连接的 PPTP 服务器的 IP 地址“ 202.101.35.218 ”，单击“ 下一步 ”。
8） 单击“ 完成 ”。
9） 双击“ pptp ” 连接，在 pptp 连接窗口，单击“ 属性 ”。
10） 选择“ 安全 ” 属性页面，选择“ 高级（自定义设置）”，单击“ 设置 ”。
11） 在“ 数据加密 ” 中选择“ 可选加密（没有加密也可以连接）”。
12） 在“ 允许这些协议 ” 选中“ 不加密的密码（PAP）”、“ 质询握手身份验证协议（CHAP）”、“ Microsoft CHAP（MS-CHAP）”，单击“ 确定 ”。
13） 选择“ 网络 ” 属性页面，在“ VPN 类型 ” 选择“ PPTP VPN ”。
14） 确认“ Internet 协议（TCP/IP）” 被选中。
15） 确认“ NWLink IPX/SPX/NetBIOS Compatible Transport Prococol ”、“ 微软网络文件和打印共享 ”、“ 微软网络客户 ” 协议没有被选中。
16） 单击“ 确定 ”，保存所做的修改。

2. 使用 PPTP 隧道连接到 HiPER PPTP 服务器：
   1） 确认计算机已经连接到 Internet（可能是拨号连接或者是固定 IP 接入）。
   2） 启动前面步骤中创建的“ pptp ” 拨号连接。
   3） 输入的 pptp 用户名“ vpn_mobile ” 和密码“ vpntest ”。
   4） 单击“ 连接 ”。
   5） 连接成功后，在 MS-DOS 方式下输入“ ipconfig ”，可以看到一个在 PPTP 服务器地址池中的地址，就是 PPTP 服务器分配给本机的 IP 地址。

5.3.1.5 相关状态信息

在 ***VPN 配置—>PPTP 和 L2TP*** 的“ PPTP/L2TP 信息列表 ”，检查 HiPER（PPTP 服务器）连接后的相关状态信息，如表 5-10、表 5-11 所示。

PPTP/L2TP 信息列表 2/6

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

	设置名	用户名	允许	会话状态	远端网关	远端内网地址	使用时间
☐	vpn_mobile	vpn_mobile	☑	已连接	192.168.123.13	192.168.210.34	00:00:00:5
☐	vpn_bj	vpn_bj	☑	已连接	202.101.35.217	192.168.16.0	00:00:14:5

表 5-10 HiPER 作为 PPTP 服务器 — PPTP/L2TP 信息列表

PPTP/L2TP 信息列表 2/6

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

	使用时间	空闲时间	出流量	入流量	业务类型	协议类型	虚接口地址	是否加密
	00:00:00:54	00:00:00:21	1269	4110	VPN接入	PPTP	10.10.10.11	否
	00:00:14:59	00:00:14:59	16385	16390	VPN接入	PPTP	10.10.10.10	否

表 5-11 HiPER 作为 PPTP 服务器 — PPTP/L2TP 信息列表（续表 5-10）

当 PPTP 客户端成功连接到 PPTP 服务器之后，“ 会话状态 ” 由“ 关闭 ” 变成“ 已连接 ”，“ 协议类型 ” 显示为“ PPTP ”。同时“ 虚接口地址 ” 显示为分配给 PPTP 客户端的 IP 地址。此时“ 使用时间 ” 开始计时，如果隧道有数据流量，那么“ 出流量 ” 和“ 入流量 ” 则开始计数。如果隧道没有数据流量，那么“ 空闲时间 ” 开始计时。

5.3.2 配置 HiPER 作为 PPTP 客户端

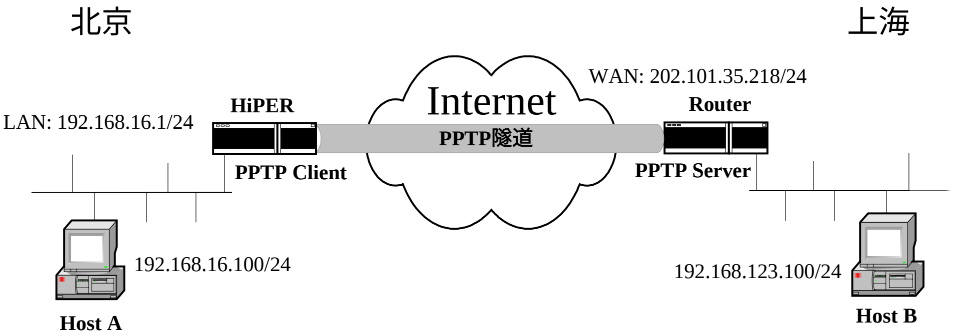


图 5-34 方案——HiPER 作为 PPTP 客户端

在本方案中，某公司总部在上海。在北京有一个分公司希望可以实现两地局域网内部资源的相互访问。

本方案使用 PPTP 协议建立 VPN 隧道，在上海公司总部使用任意品牌的标准 VPN 路由器（推荐使用 HiPER VPN 网关）PPTP 服务器，在北京分公司使用 HiPER VPN 网关作为 PPTP 客户端。地址如下：

上海（PPTP 服务器）：

局域网网段 IP 地址：192.168.123.0/24；

路由器的 LAN 口 IP 地址：192.168.123.1/24；

路由器的 WAN 口 IP 地址：202.101.35.218/24；

北京（PPTP 客户端）：

局域网网段 IP 地址：192.168.16.0/24；

HiPER 的 LAN 口 IP 地址：192.168.16.1/24；

5.3.2.1 配置 HiPER 作为 PPTP 客户端（LAN 到 LAN）

在 ***VPN 配置—>PPTP 和 L2TP*** 中，选择 " 添加 " 选项，然后在配置参数项中依次输入以下内容：

" 设置名 "：vpn_sh

" 业务类型 "：拨出（客户端）

" 用户名 "：vpn_bj

" 协议类型 "：PPTP

" 密码 "：vpntest

" 确认密码 "：vpntest

" 密码验证方式 "：PAP

" 远端内网 IP 地址 "：192.168.123.1（VPN 隧道对端局域网所使用的 IP 地址）

" 远端内网子网掩码 "：255.255.255.0

" 隧道服务器地址(名) "：202.101.35.218

再单击 " 保存 " 按钮。

5.3.2.2 配置 HiPER 作为 PPTP 服务器（LAN 到 LAN）

配置同章节 5.3.1.1 " 配置 HiPER 作为 PPTP 服务器 "。

5.3.2.3 配置 Windows 2000 Server 作为 PPTP 服务器（LAN 到 LAN）

按照以下步骤配置 Windows 2000 Server 计算机，使其成为 PPTP 服务器。

1. 设置 " 路由和远程访问 " 服务：
   1）进入 Windows 2000 Server 的 " 开始 " → " 程序 " → " 管理工具 " → " 路由和远程访问 " 配置界面，如图 5-35 所示。

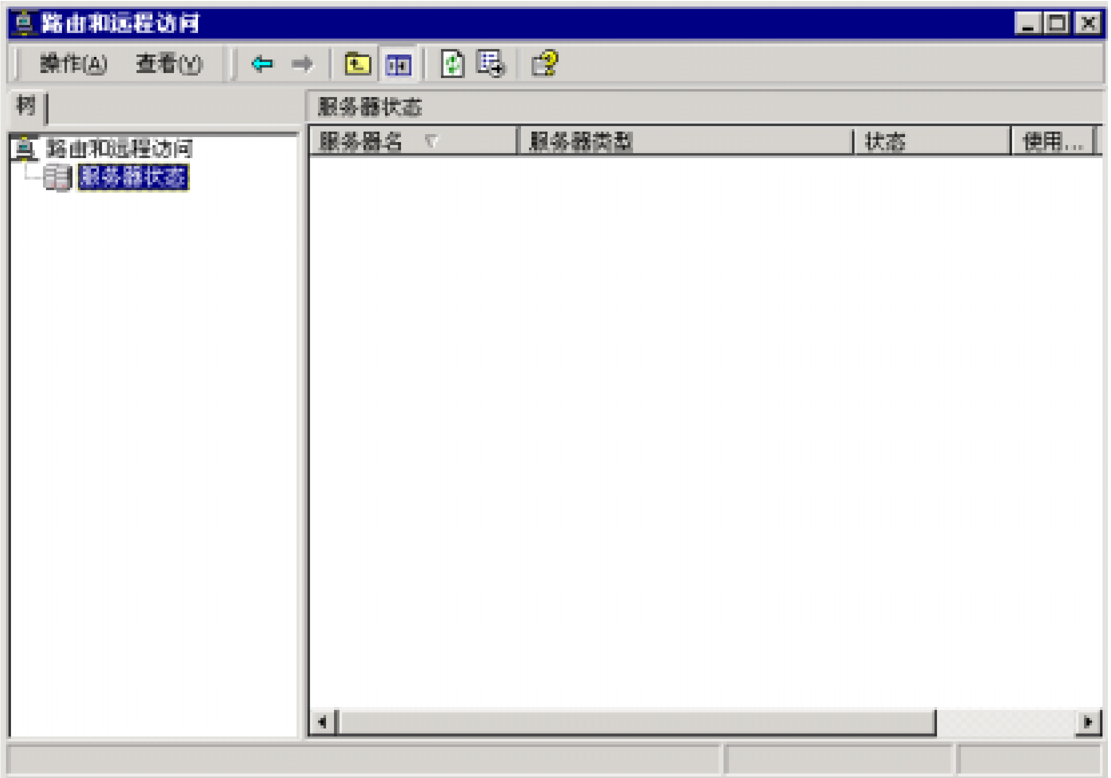


图 5-35 路由和远程访问界面一

   2）择 " 服务器状态 "，单击鼠标右键，选择 " 添加服务器 "；
   3）选择 " 这台计算机 "，单击确定，进入如图 5-36 所示界面；

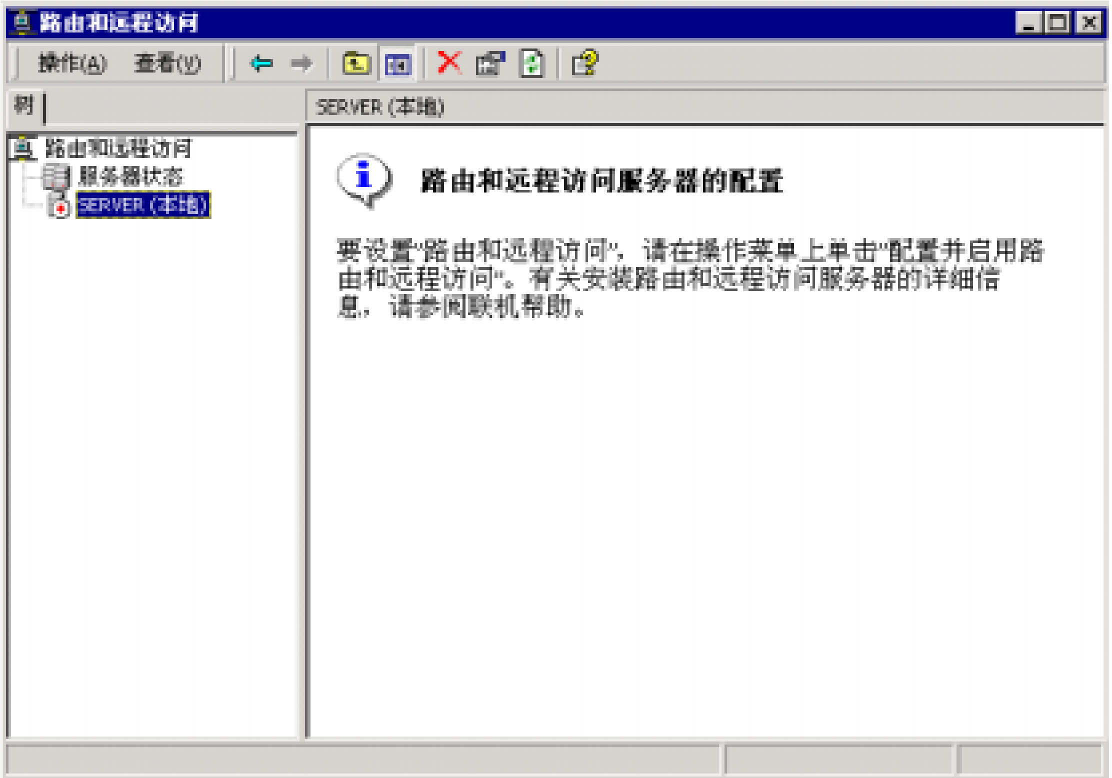


图 5-36 路由和远程访问界面二

4） 选择上一步添加的计算机，单击鼠标右键，选择“ 配置和启用路由和远程访问 ”。
5） 单击“ 下一步 ”。
6） 选择“ 手动配置服务器 ”，单击“ 下一步 ”。
7） 单击“ 完成 ”。
8） 单击“ 是 ”，以开启“ 路由和远程访问 ” 服务，如图 5-37。

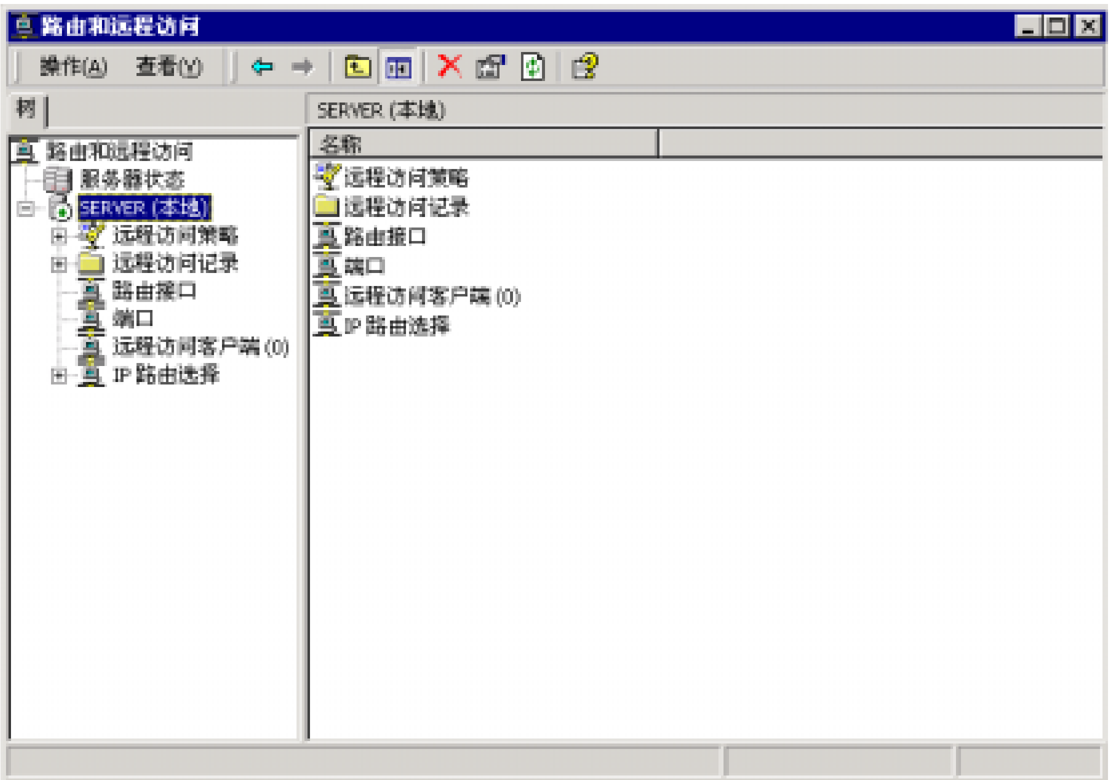


图 5-37 路由和远程访问界面三

9） 选择“SERVER”，单击鼠标右键，选择“属性”。

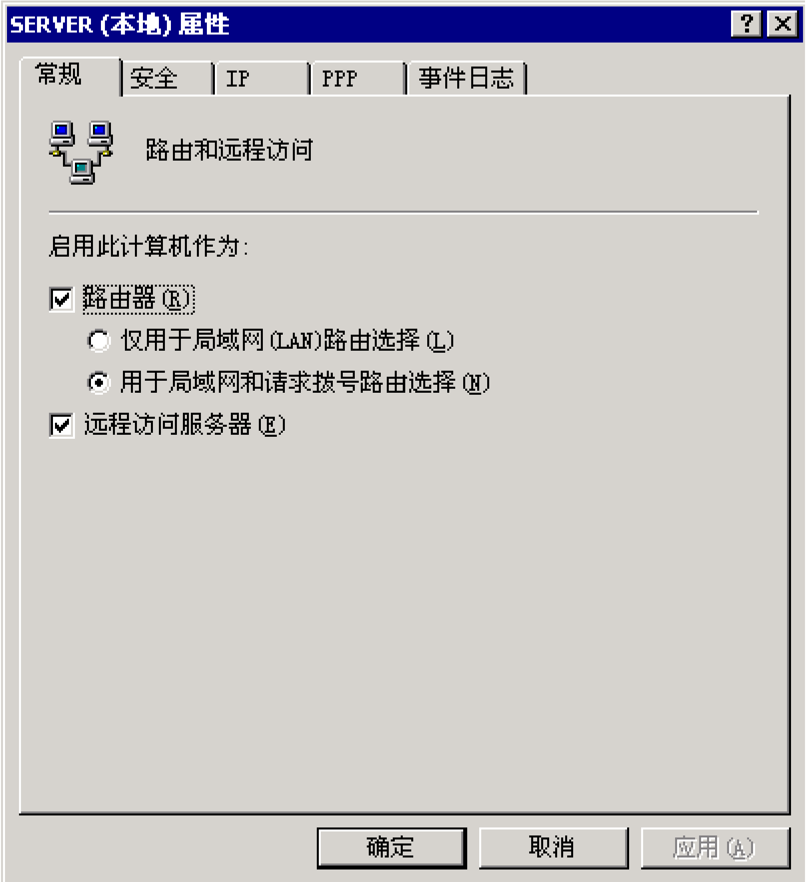


图 5-38 路由和远程访问界面四

10）进入“常规”属性页面（如图 5-38 所示），在“启用此计算机作为”选中“路由器”、“用于局域网和请求拨号路由选择”、“远程访问服务器”。

11）进入“安全”属性页面，在“验证提供程序”，选择“Windows 身份验证”，单击“身份验证方法”，进入如图 5-39 所示界面。

12）选中“Microsoft 加密身份验证（MS-CHAP）”、“加密身份验证（CHAP）”、“不加密的密码（PAP）”，单击“确定”。

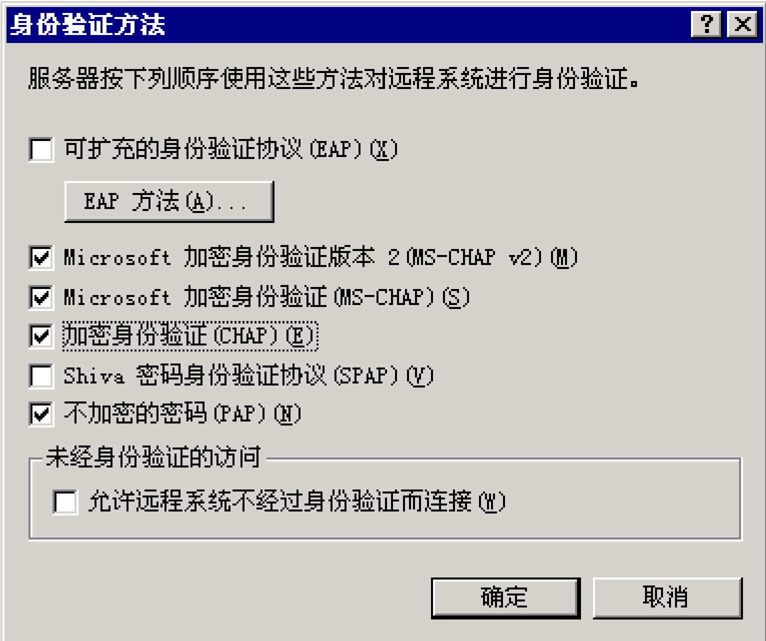


图 5-39 身份验证方法界面

13）进入“IP”属性页面，选中“启用 IP 路由”，选中“允许基于 IP 的远程访问和请求拨号连接”。选择“静态地址池”，单击“添加”，进入如图 5-40 所示界面。

14）输入起始 IP 地址“192.168.123.201”，地址数“50”（输入 Windows 2000 Server 局域网端口所在网段一段空闲的 IP 地址），单击确定。

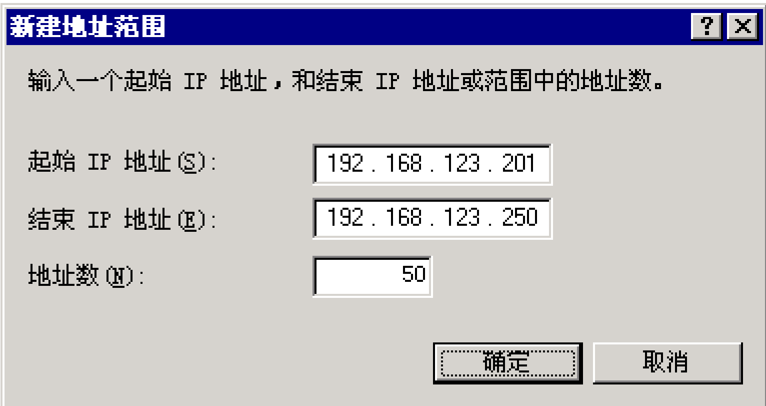


图 5-40 新建地址范围界面

15）在“适配器”，选中“允许 RAS 选择适配器”（如果计算机只安装了一块网卡，看不到此选项），单击“确定”。

16）选择“远程访问策略”，单击鼠标右键，选择“新建远程访问策略”。

17）填入远程访问策略的名称“vpn”，单击“下一步”。

18）单击“添加”。

19）选中“NAS-Port-Type”，单击“添加”，如图 5-41 所示。

20）将“可用类型”“Virtual（VPN）”添加到“选择的类型”中，单击“确定”。

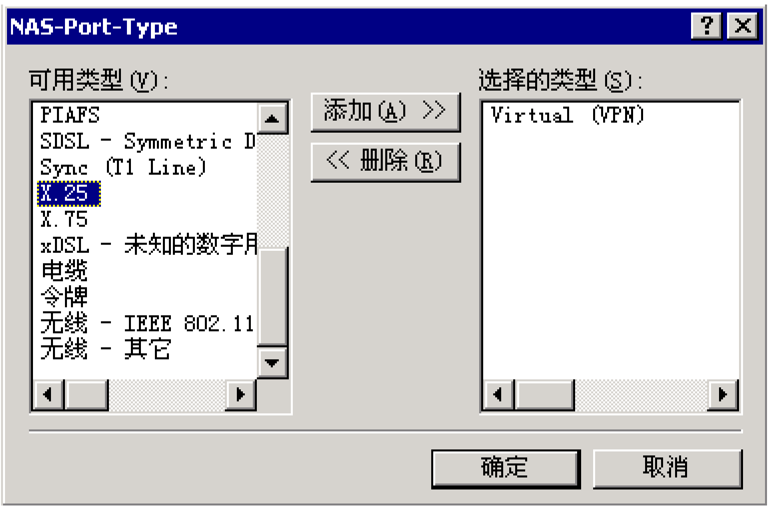


图 5-41 NAS-Port-Type 界面

21）单击“下一步”。
22）选中“授予远程访问权限”，单击“下一步”。
23）单击“编辑配置文件”，进入如图 5-42 所示界面。
24）在“身份验证”属性页面，选中“Microsoft 加密身份验证（MS-CHAP）”、“加密身份验证（CHAP）”、“未加密的密码（PAP，SPAP）”，单击确定。

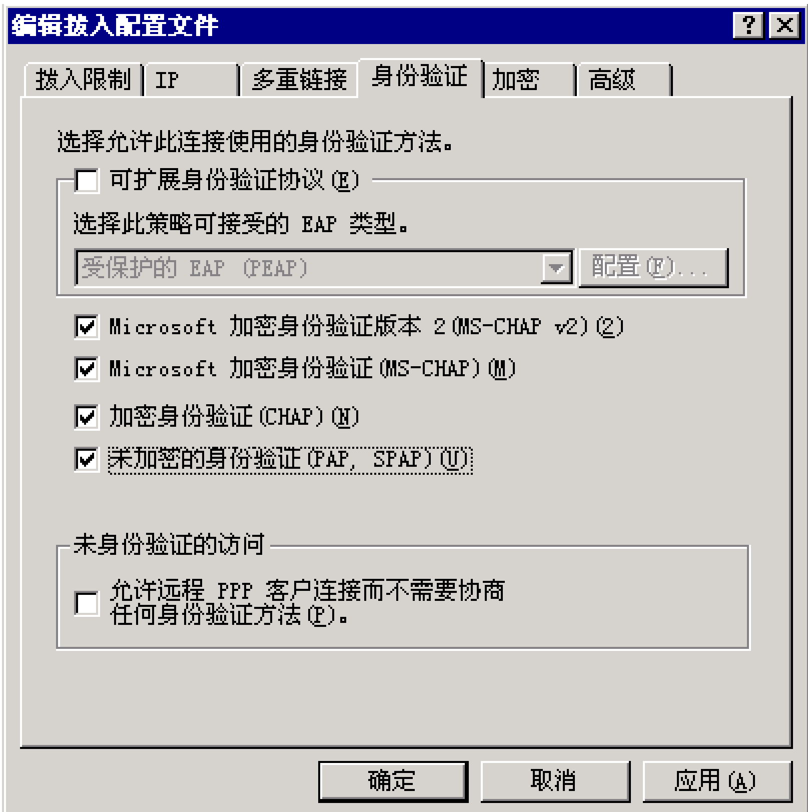


图 5-42 编辑拨入配置文件界面

25）单击“确定”。
26）选中“端口”，单击鼠标右键，选择“属性”。
27）选中“WAN 微型端口（PPTP）”，单击“配置”，进入如图 5-43 所示界面。

28）根据实际 PPTP 客户端的数量，调整“ 最多端口数 ”，单击确定。

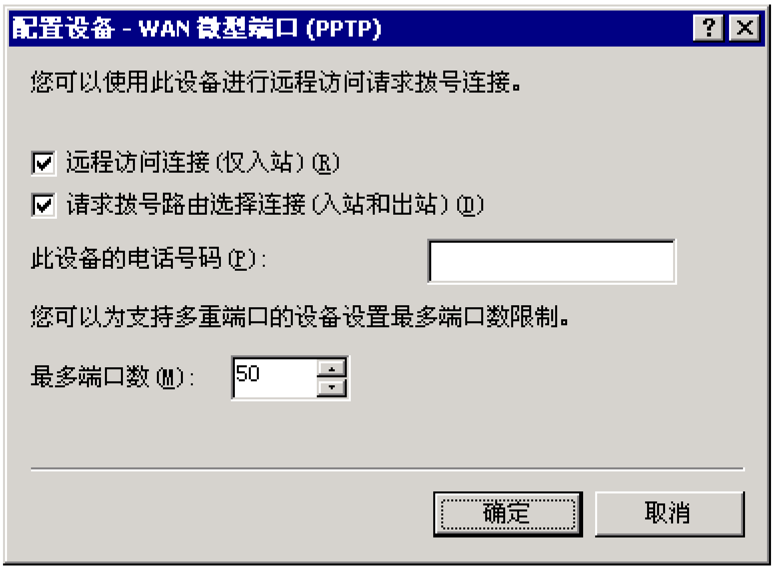


图 5-43 配置设备界面

29）路由和远程访问服务配置完成。

3. 配置拨入的 VPN 用户帐号：

1）进入 Windows 2000 Server 的开始→程序→管理工具→计算机管理（注意：如果配置了 Windows 2000 Server 成为域控制器，可以在 Active Directory 的用户管理中添加用户帐号）。

2）选中“ 本地用户和组 ”→“ 用户 ”，单击鼠标右键，选择“ 新用户 ”，进入如图 5-44 所示界面。

3）首先依次填入以下参数，然后单击“ 创建 ”按钮。

“ 用户名 ”：vpn_bj
“ 密码 ”：vpntest
“ 确认密码 ”：vpntest
“ 用户下次登录时须更改密码 ”：取消选中
“ 用户不能更改密码 ”：选中
“ 密码永不过期 ”：选中

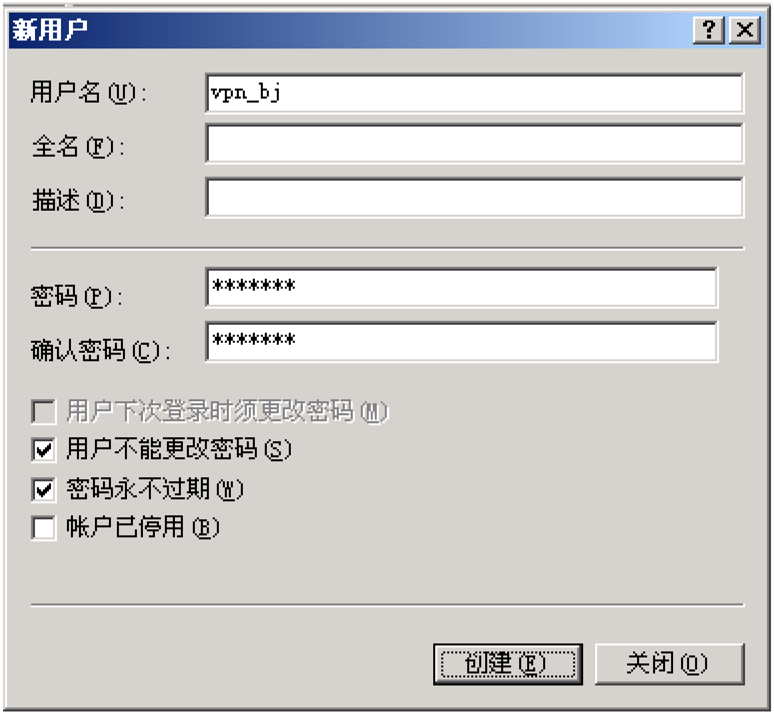


图 5-44 新用户界面

4） 选中上一步新建的 “ vpn_bj ” 用户，单击鼠标右键，选择属性。
5） 在 “ 拨入 ” 属性页面，在 “ 远程访问权限 ” 选择 “ 通过远程访问策略控制访问 ”。
6） 在 “ 回拨选项 ” 选择 “ 不回拨 ”。
7） 选中 “ 分配静态 IP 地址 ”，从地址池中选择一个 IP 地址 192.168.123.240（在 “ 路由和远程访问 ” 中第 14 步配置）作为分配给此帐号的 IP 地址。
8） 选中 “ 应用静态路由 ”。
9） 单击 “ 添加路由 ”，进入如图 5-45 所示界面。
10） 填入北京路由器局域网的网段，目标：192.168.16.0，网络掩码：255.255.255.0，跃点数 “ 1 ”，单击确定。

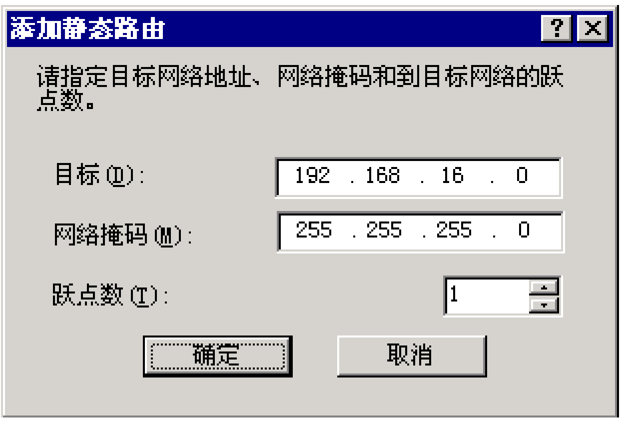


图 5-45 添加静态路由界面

11） 单击两次 “ 确定 ”。
12） VPN 用户帐号配置完成。

4. 查看 PPTP 隧道连接状态：

进入 Windows 2000 Server 的 “ 开始 ” → “ 程序 ” → “ 管理工具 ” → “ 路由和远程访问 ”，

选中“远程访问客户端”，可以在窗口右侧看到拨入的用户信息。

双击“拨入的用户”，可以查看一些实时的 PPTP 隧道连接信息，如图 5-46 所示。

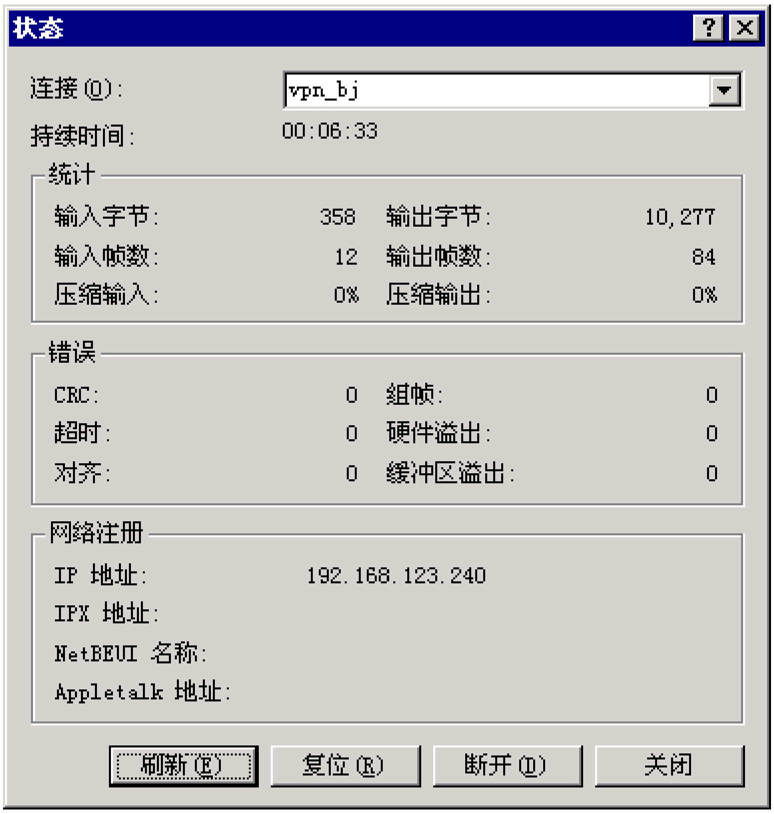


图 5-46 VPN 状态信息界面

5.3.2.4 配置 Cisco 路由器作为 PPTP 服务器（LAN 到 LAN）

按照以下步骤配置 Cisco 路由器，使其成为 PPTP 服务器。Cisco 在做 VPN 接入的时候，必须配置 Radius Server 为 Cisco 验证用户身份、添加用户路由。

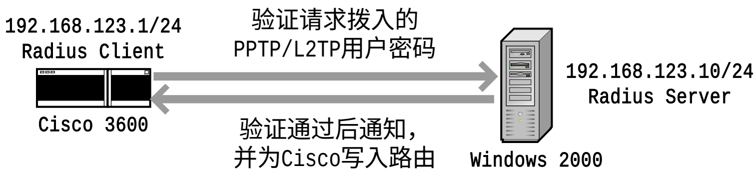


图 5-47 方案——Cisco 路由器作为 PPTP 服务器

1. 配置 Cisco 成为 PPTP 服务器

//配置 PPTP 服务器的全局参数

vpdn enable

vpdn-group 1

accept-dialin

protocol PPTP

virtual-template 1

local name runway

lcp renegotiation always

//配置 PPTP 服务器的 Virtual-Template（IP 地址 unnumbered 路由器 WAN 口）

interface Virtual-Template1
ip unnumbered Ethernet0/0
peer default ip address pool default
ppp authentication pap

//配置 PPTP 地址池

ip local pool default 10.0.0.1 10.0.0.254

2. 配置 Cisco 成为 Radius Client

//配置一个 Cisco 访问帐号

username admin password admin321

//配置 Cisco 的 AAA

aaa new-model
aaa authentication login default local
aaa authentication ppp default group radius local
aaa authorization network default group radius local
aaa accounting exec default start-stop group radius
aaa accounting network default start-stop group radius

//配置 Radius 服务器的 IP 地址和口令

radius-server host 192.168.123.10 auth-port 1812 acct-port 1813
radius-server retransmit 3
radius-server key testing123

3. 在 Windows 2000 Server 上安装“Internet 验证服务”：
   1） 进入 Windows 2000 Server 的“开始”→“设置”→“控制面板”→“添加/删除程序”。
   2） 选择“添加/删除 Windows 组件”。
   3） 选择“组件”→“网络服务”→“Internet 验证服务”，单击“确定”。
   4） 如果需要的话插入 Microsoft Windows 2000 Server 安装软盘或者 CD。

4. 配置 Windows 2000 Server 的 Internet 验证服务”服务：
   1） 进入 Windows 2000 Server 的“开始”→“程序”→“管理工具”→ “Internet 验证服务”配置界面，如图 5-48 所示。

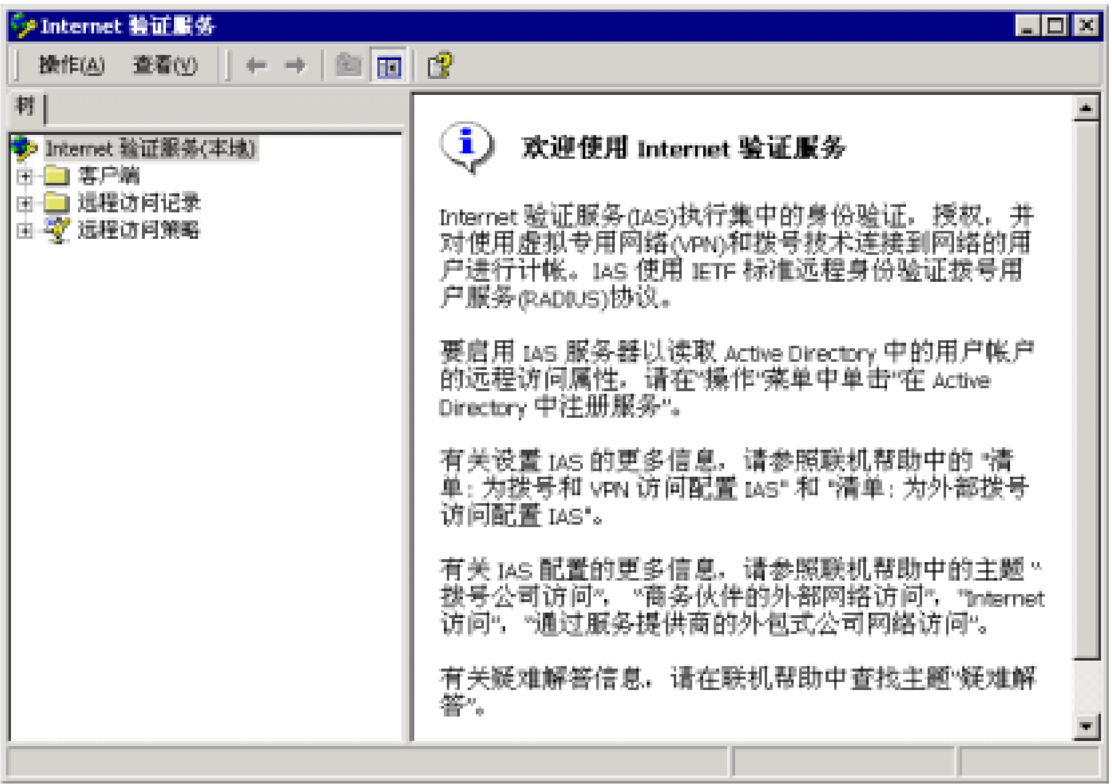


图 5-48 Internet 验证服务界面

2） 选中“ 客户端 ”，单击鼠标右键，选择“ 新建客户端 ”。
3） “ 为客户端输入一个好记的名称 ” 填入“ cisco ”，“ 协议 ” 选择“ RADIUS ”，单击“ 下一步 ”，进入如图 5-49 所示界面。
4） 填入“ 客户端地址（IP 或 DNS）”：192.168.123.1 ;“ 客户端-供应商 ”：RADIUS Standard ;“ 共享的机密 ”：testing123 ;“ 确认共享的机密 ”：testing123。确认“ 客户端必须总是在请求中发送签名属性 ” 没有被选中，然后单击“ 完成 ”。

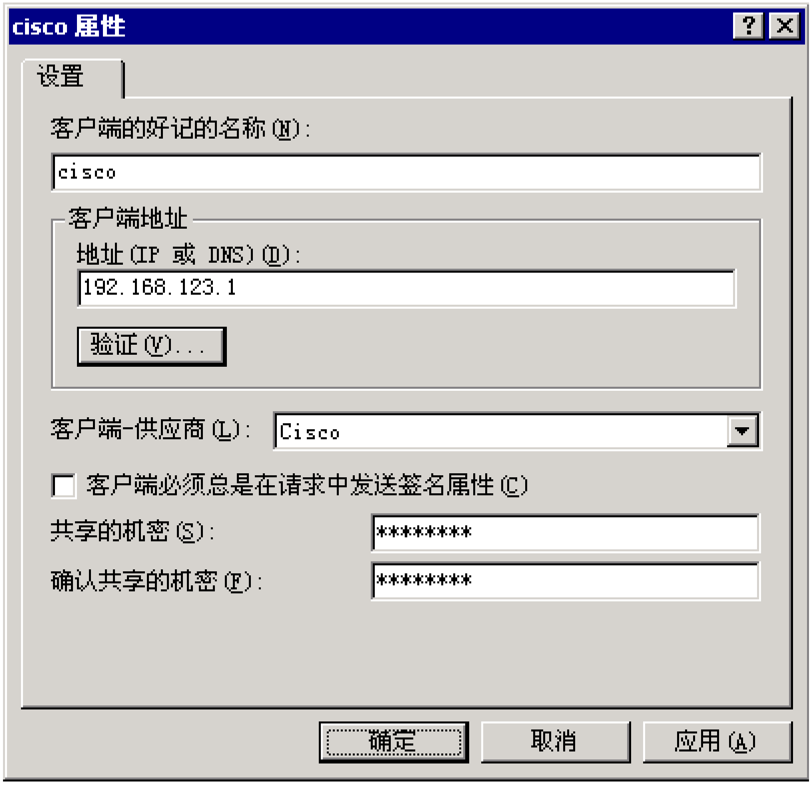


图 5-49 cisco 属性界面

5） 选择“ 远程访问策略 ”，单击鼠标右键，选择“ 新建远程访问策略 ”。

6） 填入远程访问策略的名称“ cisco ”，单击“ 下一步 ”。

7） 单击“ 添加 ”，进入如图 5-50 所示界面。

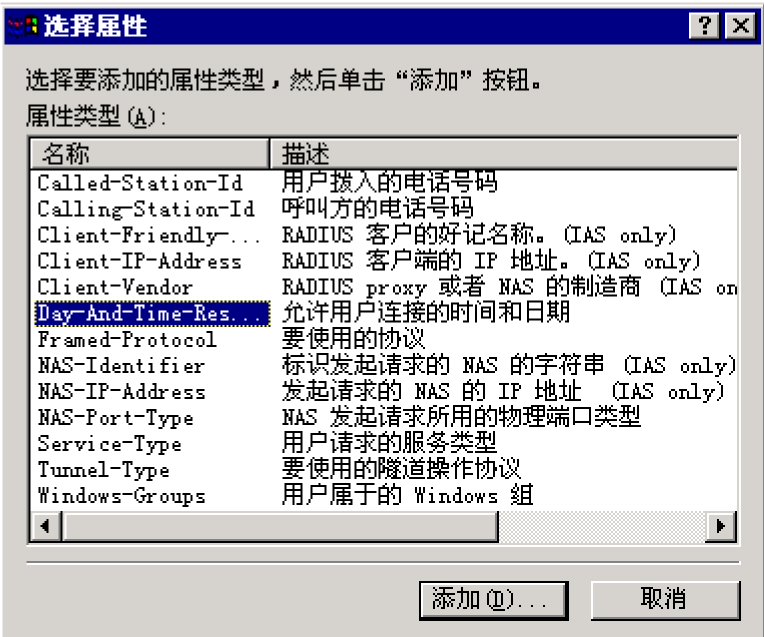


图 5-50 选择属性界面

8） 选中“ Day-And-Time-Restrictions ”，单击“ 添加 ”，进入如图 5-51 所示界面。

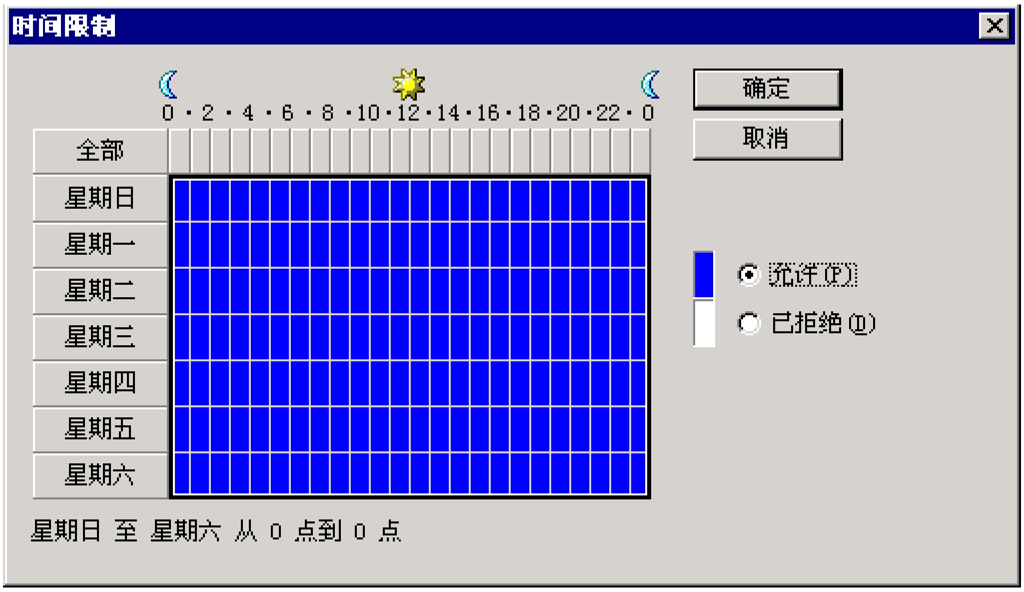


图 5-51 选择属性界面

9）选择“允许”，单击“确定”。

10）选中“授予远程访问权限”，单击“下一步”。

11）单击“编辑配置文件”。

12）在“身份验证”属性页面（如图 5-52 所示），选中“Microsoft 加密身份验证（MS-CHAP）”、“加密身份验证（CHAP）”、“未加密的密码（PAP，SPAP）”，单击“确定”。

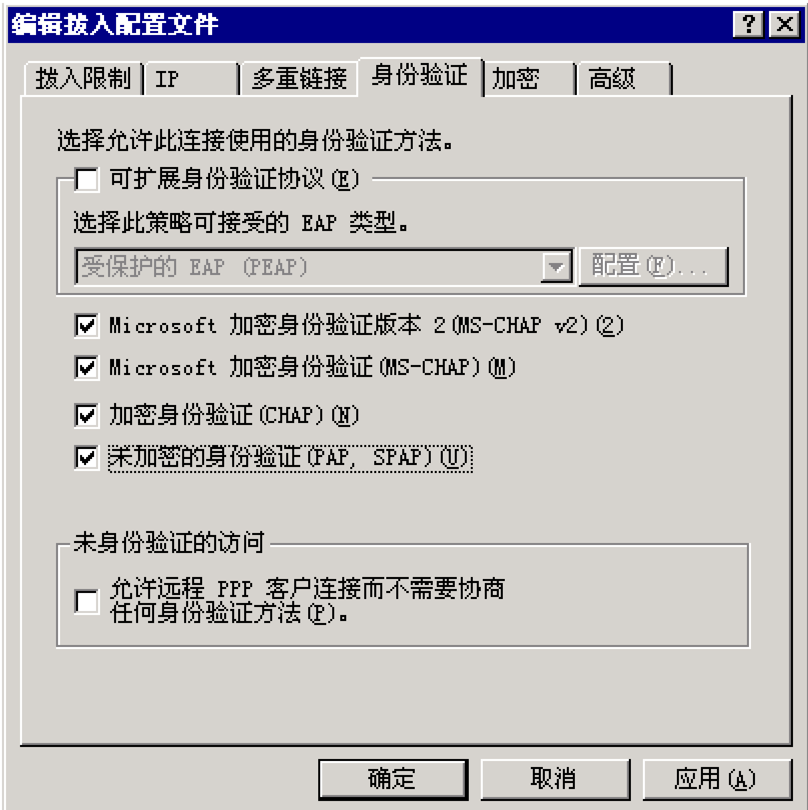


图 5-52 编辑拨入配置文件界面

13）单击“确定”。

5. 配置拨入的 VPN 用户帐号：
   1） 进入 Windows 2000 Server 的 " 开始 " → " 程序 " → " 管理工具 " → " 计算机管理 "（注意：如果配置了 Windows 2000 Server 成为域控制器，可以在 Active Directory 的用户管理中添加用户帐号）。
   2） 选中 " 本地用户和组 " → " 用户 "，单击鼠标右键，选择 " 新用户 "，进入如图 5-53 所示界面。
   3） 首先依次填入以下参数，然后单击 " 创建 " 按钮。
   " 用户名 "：vpn_bj
   " 密码 "：vpntest
   " 确认密码 "：vpntest
   " 用户下次登录时须更改密码 "：取消选中
   " 用户不能更改密码 "：选中
   " 密码永不过期 "：选中

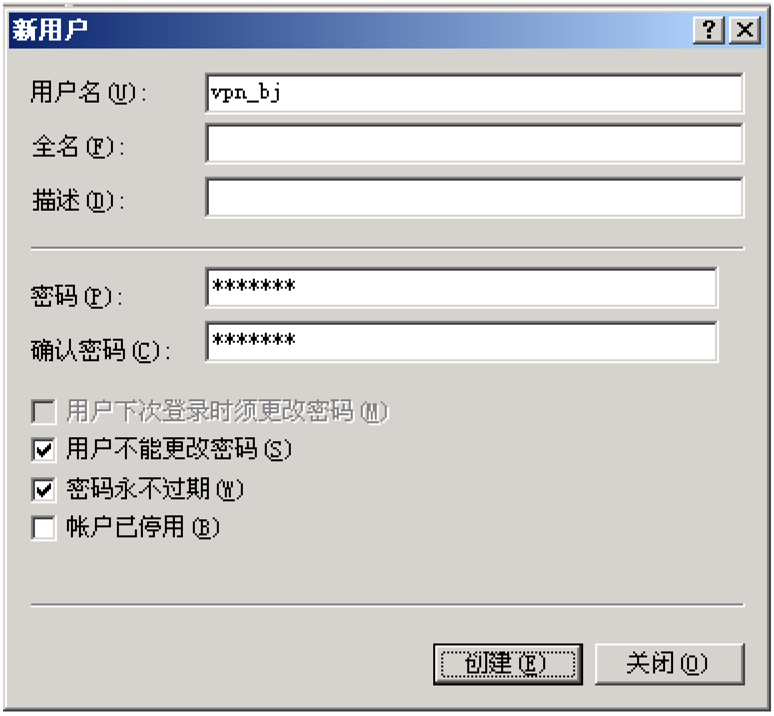


图 5-53 新用户界面

   4） 选中上一步新建的 " vpn_bj " 用户，单击鼠标右键，选择 " 属性 "。
   5） 在 " 拨入 " 属性页面，在 " 远程访问权限 " 选择 " 通过远程访问策略控制访问 "。
   6） 在 " 回拨选项 " 选择 " 不回拨 "。
   7） 选中 " 分配静态 IP 地址 "，从 Cisco VPN 地址池中选择一个 IP 地址 10.0.0.123（在 " 路由和远程访问 " 中第 14 步配置）作为分配给此帐号的 IP 地址。
   8） 选中 " 应用静态路由 "。
   9） 单击 " 添加路由 "，进入如图 5-54 所示界面。
   10） 填入北京路由器局域网的网段，目标：192.168.16.0，网络掩码：255.255.255.0，跃点数 " 1 "，单击 " 确定 "。

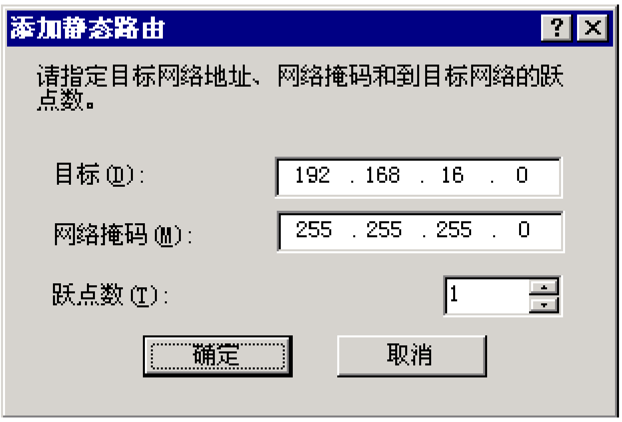


图 5-54 添加静态路由界面

11） 单击两次“ 确定 ”。

12） VPN 用户帐号配置完成。

5.3.2.5 配置 Fortigate 防火墙作为 PPTP 服务器（LAN 到 LAN）

按照以下步骤配置 Fortigate 防火墙（注：本手册使用的是 Fortigate 300A 产品），使其成为 PPTP 客户端。

1. 配置用户：

   1） 进入 Fortigate 防火墙的的“ 设置用户 ”→“ 本地 ”页面，单击“ 新建 ”，进入如图 5-55 所示界面。

   2） 输入 L2TP VPN 的“ 用户名称 ”为“ vpn_bj ”；“ 输入密码 ”为“ vpntest ”，单击“ OK ”。

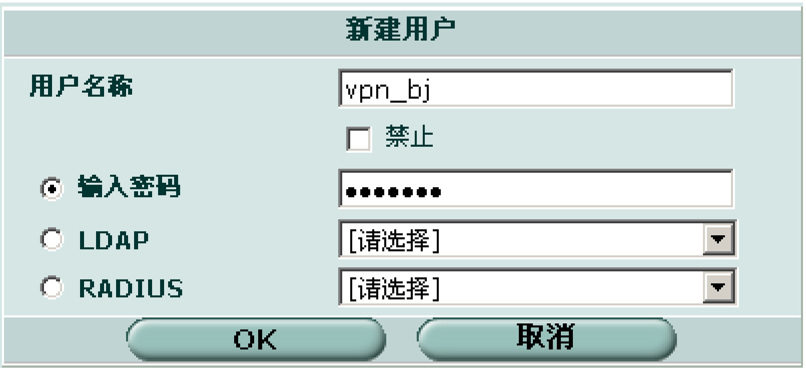


图 5-55 新建用户界面

2. 配置用户组：

   1） 进入 Fortigate 防火墙的“ 设置用户 ”→“ 用户组 ”，单击“ 新建 ”，进入如图 5-56 所示界面。

   2） 填入“ 组名 ”为“ pptp ”，将“ vpn_bj ”用户添加到组员中去。单击“ OK ”。

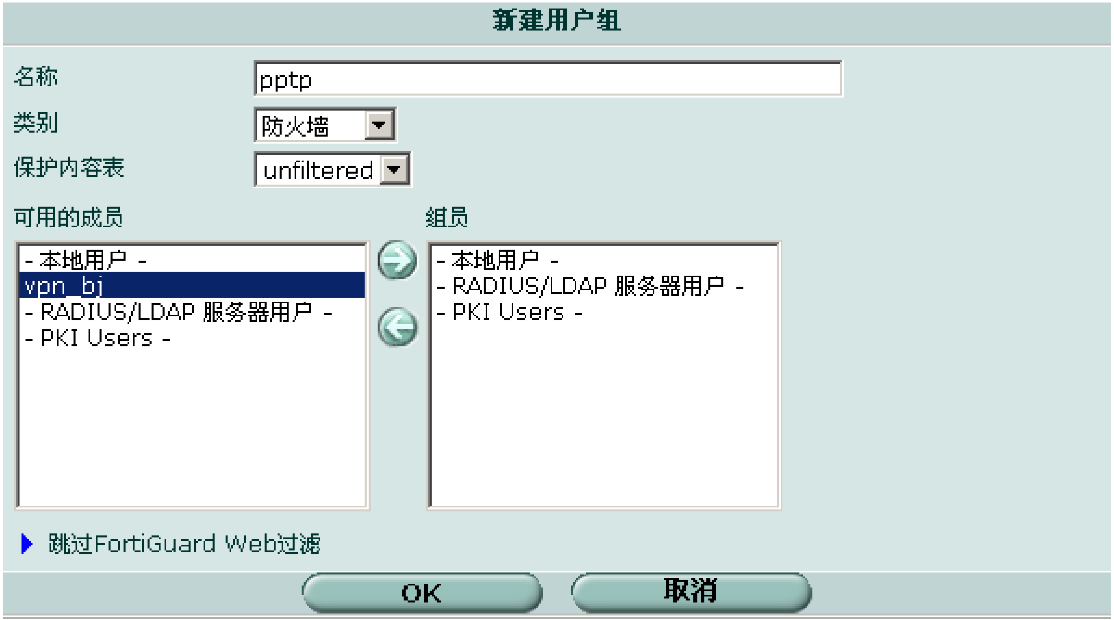


图 5-56 新建用户组界面

3. 启用 PPTP：
   1） 进入 Fortigate 防火墙的→ " 虚拟专网 " → " PPTP "，进入如图 5-57 所示界面。
   2） 选中 " 启用 PPTP "，设置 " 起始 IP " 为 10.10.10.1，" 终止 IP " 为 10.10.10.10（任意其他网段一段空闲的 IP 地址），" 用户组 " 选择上一步新建的 " pptp " 用户组，单击 " 应用 " 按钮。



图 5-57 启用 PPTP 界面

4. 设置防火墙策略：
   1） 进入 Fortigate 防火墙的 " 防火墙 " → " 地址 " 页面。
   2） 单击 " 新建 "，进入如图 5-58 所示界面。
   3） 设置地址名称为 " lan123 "，类型为 " 子网/IP 范围 "，" 子网/IP 范围 " 为 Fortigate 防火墙的局域网网段 " 192.168.123.0/255.255.255.0 "，接口选择用于连接局域网的端口，本例选择 " port1 口 "，单击 " OK " 按钮。



图 5-58 新设地址界面一

4） 单击“新建”，进入如图 5-59 所示界面。
5） 设置地址名称为“vpn20”，类型为“子网/IP 范围”“子网/IP 范围”为第 3 步设置的 Fortigate 防火墙的 PPTP 地址池所在的网段“10.10.10.0/255.255.255.0”，接口选择为用于连接外网的端口（即 WAN1），本例中选择“port 6”，单击“OK”。

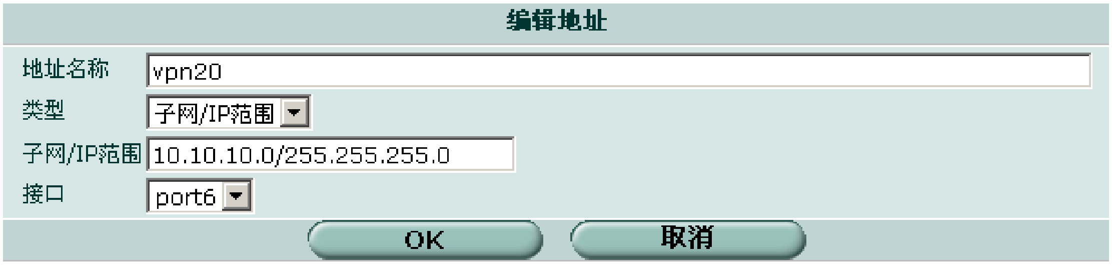


图 5-59 新设地址界面二

6） 进入 Fortigate 防火墙的“防火墙”→“策略”页面。
7） 单击“新建”，进入如图 5-60 所示界面。
8） “源接口/区”选择“port6”,“源地址”选择上面设定的“vpn20”地址段，“目的接口/区”选择“port1”，“目的地址”选择上面设定的“lan123”地址段，完成其他防火墙设置策略后单击“OK”。

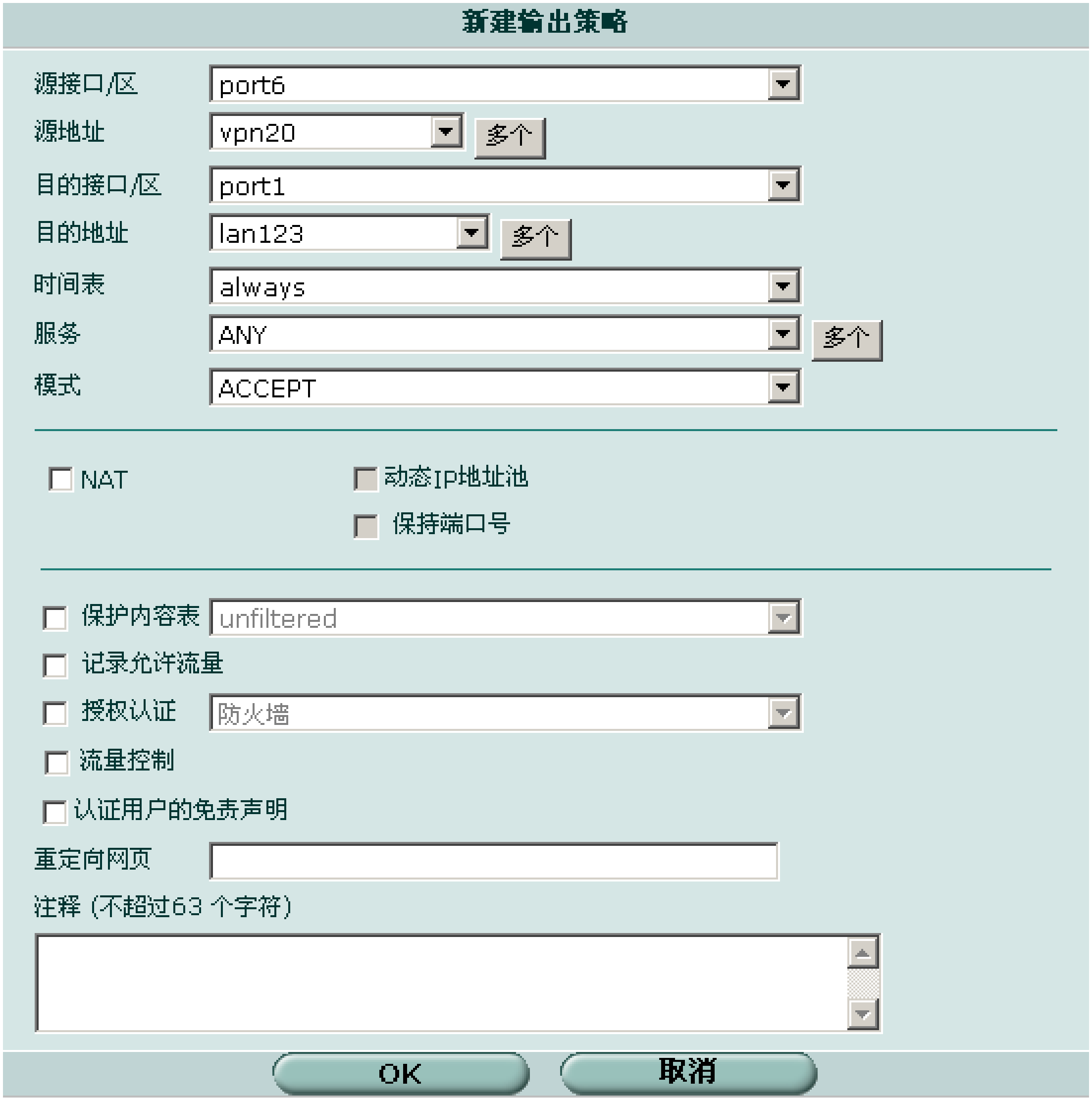


图 5-60 新建输出策略界面

提示：Fortigate 防火墙只支持移动用户的接入，如果想实现一个局域网通过路由器连接到 Fortigate 防火墙，就必须在 PPTP/L2TP 隧道连接上启用 NAT，可以参考章节 5.4.1 里面的设置，但是这样只能是实现 PPTP/L2TP 客户端局域网到 Fortigate 防火墙端局域网的单向访问。

5.3.2.6 相关状态信息

在 ***VPN 配置—>PPTP 和 L2TP*** 的“ PPTP/L2TP 信息列表 ”中，检查 HiPER VPN 网关（作为 PPTP 客户端）连接前后的相关状态信息，如表 5-12、表 5-13 所示。


PPTP/L2TP 信息列表 1/16

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

	设置名	用户名	允许	会话状态	远端网关	远端内网地址	使用时间
☐	vpn_sh	vpn_bj	☑	已连接	202.101.35.218	192.168.123.1	00:00:00:04

表 5-12 HiPER 作为 L2TP 客户端 — PPTP/L2TP 信息列表

PPTP/L2TP 信息列表 1/16

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

使用时间	空闲时间	出流量	入流量	业务类型	协议类型	虚接口地址	是否加密
0:00:00:04	00:00:00:04	370	554	VPN拨出	PPTP	10.10.10.10	否

表 5-13 HiPER 作为 L2TP 客户端 — PPTP/L2TP 信息列表（续表 5-12）

当 PPTP 客户端成功连接到 PPTP 服务器之后，“ 会话状态 ”由“ 关闭 ”变成“ 已连接 ”，同时获得 PPTP 服务器分配的“ 虚接口地址 ”为“ 10.10.10.10 ”。此时“ 使用时间 ”开始计时，如果隧道有数据流量，那么“ 出流量 ”和“ 入流量 ”开始计数。如果隧道没有数据流量，那么“ 空闲时间 ” 开始计时。

5.4 HiPER 的 PPTP/L2TP 的综合应用

5.4.1 使用移动用户的帐号实现 LAN 到 LAN 的连接

HiPER VPN 网关作为 PPTP/L2TP 服务器使用时，一般都有两种用户帐号：一种是移动用户帐号，用来让个人用户连接到 PPTP/L2TP 服务器，这种情况下 PPTP/L2TP 服务器中不需要配置到个人用户的路由；一种是 LAN 到 LAN 的帐号，用来实现 PPTP/L2TP 隧道两端局域网的相互连接，这种情况下 PPTP/L2TP 隧道两端的设备都要配置到对端的路由。

然而在下面这些情况下，需要在 PPTP/L2TP 隧道连接上启用 NAT：

1. PPTP/L2TP 客户端使用移动用户的帐号连接 PPTP/L2TP 服务器，实现整个局域网到 PPTP/L2TP 服务器端局域网的连接；
2. PPTP/L2TP 隧道连通之后，需要实现 PPTP/L2TP 客户端到 PPTP/L2TP 服务器的单向访问；
3. PPTP/L2TP 服务器不能配置到 PPTP/L2TP 客户端的路由（比如配置 Cisco 路由器做 PPTP/L2TP 服务器的时候，无法配置 Radius 服务器）；

方法：配置 HiPER VPN 网关成为 PPTP/L2TP 客户端时，在 ***VPN 配置—>PPTP 和 L2TP*** 的高级选项中，选中“ 启用 NAT ”，如图 5-61。

启用NAT ☑

图 5-61 启用 NAT

在 PPTP/L2TP 隧道连接成功之后，在***系统状态—>路由和端口信息***的“ 路由表信息列表 ”中，可以发现到其对端服务器的路由中，已经启用了 NAT（到目的地址 192.168.123.0/24 的路由状态可见“ N ”），如表 5-14 所示。

路由表信息列表 22/22

1/3 第一页 上一页 下一页 最后页 前往 第 页 搜索

目的地址	网关地址	接口号	路由状态	优先级	跳数	使用次数	使用时间
0.0.0.0/0	202.101.35.218	ie1	lugpaN	60	1	0	84
10.10.10.10/32	-	local	Ruhtp	60	0	0	84
127.0.0.0/8	-	bhole0	cup	20	0	0	411664
127.0.0.1/32	-	local	cuhp	20	0	0	411664
127.0.0.2/32	-	reject0	cuhp	20	0	0	411664
127.0.0.3/32	-	bhole0	cuhp	20	0	0	411664
192.168.1.1/32	-	local	cuhp	20	0	684	411662
192.168.123.0/24	10.10.10.10	ptp14	lugN	60	1	0	84
192.168.123.0/32	10.10.10.10	ptp14	lughN	60	1	0	3722
192.168.123.1/32	10.10.10.10	ptp14	lughN	60	1	0	84

表 5-14 路由表信息列表

⌖ 提示：在 PPTP/L2TP 隧道上启用了 NAT，PPTP/L2TP 隧道连通之后，只能实现 PPTP/L2TP 客户端到 PPTP/L2TP 服务器的单向访问，从 PPTP/L2TP 服务器到 PPTP/L2TP 客户端的访问将被拒绝。

5.4.2 将默认路由绑定到 PPTP/L2TP 隧道

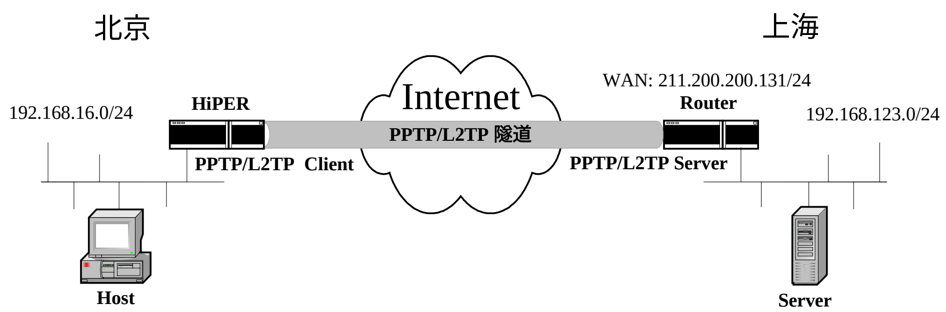


图 5-62 方案——HiPER 默认路由绑定到 VPN 隧道

如表 5-15 所示，在 HiPER VPN 网关作为 PPTP/L2TP 客户端成功连接到 PPTP/L2TP 服务器后，在其路由表（*系统状态—>路由和端口信息*的“路由表信息列表”）里面会形成两条路由，一条到 PPTP/L2TP 服务器（192.168.123.0/24）网段的路由，一条默认路由（0.0.0.0/0）。HiPER VPN 网关（PPTP/L2TP 客户端）将会根据来自本地局域网的数据包的目的地址来决定该数据包是通过默认路由从本地上网，还是通过 PPTP/L2TP 隧道到达 PPTP/L2TP 隧道远端的局域网。

路由表信息列表 22/22

1/3 第一页 上一页 下一页 最后页 前往 第 页 搜索

目的地址	网关地址	接口号	路由状态	优先级	跳数	使用次数	使用时间
0.0.0.0/0	200.200.200.173	ie1	lugpaN	60	1	886	916
10.10.10.12/32	-	local	Ruhtp	60	0	0	334
127.0.0.0/8	-	bhole0	cup	20	0	0	426172
127.0.0.1/32	-	local	cuhp	20	0	0	426172
127.0.0.2/32	-	reject0	cuhp	20	0	0	426172
127.0.0.3/32	-	bhole0	cuhp	20	0	0	426172
192.168.1.1/32	-	local	cuhp	20	0	684	426170
192.168.123.0/24	10.10.10.12	ptp1	lug	60	1	0	334
192.168.123.1/32	10.10.10.12	ptp1	lugh	60	1	0	334
192.168.16.0/24	-	ie0	cua	20	0	6168	18845

表 5-15 路由表信息列表

但是，如果希望在 PPTP/L2TP 服务器端控制 PPTP/L2TP 客户端的上网权限，就需要将 HiPER VPN 网关（PPTP/L2TP 客户端）配置成为：PPTP/L2TP 隧道连通之后所有的局域网流量（到 PPTP/L2TP 服务器端的局域网和其他网络）都经过 PPTP/L2TP 隧道转发到 PPTP/L2TP 服务器，也就是将上网的默认路由绑定到 PPTP/L2TP 隧道。

由于 HiPER VPN 网关中，上网线路以及 PPTP/L2TP 隧道的相关路由参数中，“优先级”和“断开优先级”的默认值分别为“60”、“120”；所以可以通过调高 PPTP/L2TP 隧道的路由“优先级”和“断开优先级”来实现上述目的。配置方法如下：

1. 在 HiPER VPN 网关（PPTP/L2TP 客户端）中配置到 PPTP/L2TP 服务器的路由

   1) HiPER 是固定 IP 接入

在*高级配置—>路由配置*的“路由参数设置”中，选中“添加”，在相关配置参数项中依次填入以下内容，再单击“保存”，如图 5-63 所示。

“路由设置名称”：vpn_server
“目的网络”：211.200.200.200.131（PPTP/L2TP 服务器的 IP 地址）
“网络掩码”：255.255.255.255
“网关地址”：200.200.200.173（本地固定 IP 接入的网关地址）



图 5-63 路由参数设置

   2) HiPER VPN 是 PPPoE 接入

在*高级配置—>路由配置*的“路由参数设置”中，选中“添加”，在相关配置参数项中

依次填入以下内容，再单击“保存”，如图 5-64 所示。

“路由设置名称”：vpn_server

“目的网络”：211.200.200.131（PPTP/L2TP 服务器的 IP 地址）

“网络掩码”：255.255.255.255

“绑定”：默认线路（当前 PPPoE 连接线路为默认线路）



图 5-64 路由参数设置（高级选项）

2. 在 HiPER VPN 网关（PPTP/L2TP 客户端）中配置隧道相关参数

在 ***VPN 配置—>PPTP 和 L2TP*** 中，选中“高级选项”，依次进行如下配置：

1) 将“远端内网 IP 地址”、“远端内网子网掩码”均设置成“0.0.0.0”，如图 5-65 所示。



图 5-65 PPTP/L2TP 隧道参数（远端内网 IP 地址）设置

2) 将“优先级”调高至“59”（值越小优先级越高）、“断开优先级”调高至“119”（值越小优先级越高），如图 5-66 所示。

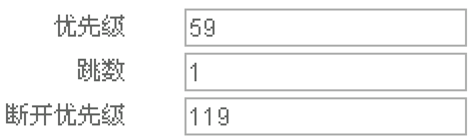


图 5-66 PPTP/L2TP 隧道参数（优先级）设置

3) 选中“高级选项”，选中“启用 NAT”，如图 5-67 所示。



图 5-67 PPTP/L2TP 隧道参数（启用 NAT）设置

4) 启用“保持连接”（PPTP/L2TP 隧道两端设备均要启用本设置），如图 5-68 所示。



图 5-68 PPTP/L2TP 隧道参数（保持连接）设置

上述配置完成后，在*系统状态—>路由和端口信息*的“路由表信息列表”中，可以查看到上网线路的路由被标记成备份状态，而 PPTP/L2TP 隧道连接成功后被作为默认路由，如

表 5-16 所示；还可以看到一条到 PPTP/L2TP 服务器的主机路由，如表 5-17 所示。

路由表信息列表 22/22

1/3 第一页 上一页 下一页 最后页 前往 第 页 搜索

目的地址	网关地址	接口号	路由状态	优先级	跳数	使用次数	使用时间
0.0.0.0/0	10.10.10.13	ptp2	lugaN	59	1	0	5
0.0.0.0/0	200.200.200.173	ie1	*lugpaN	60	1	0	8
0.0.0.0/0	-	ptpdial0	*luga	119	7	0	8
10.10.10.13/32	-	local	Ruhtp	60	0	0	5
127.0.0.0/8	-	bhole0	cup	20	0	0	427563
127.0.0.1/32	-	local	cuhp	20	0	0	427563
127.0.0.2/32	-	reject0	cuhp	20	0	0	427563
127.0.0.3/32	-	bhole0	cuhp	20	0	0	427563
192.168.1.1/32	-	local	cuhp	20	0	684	427561
192.168.16.0/24	-	ie0	cua	20	0	9350	20236

表 5-16 路由表信息列表

路由表信息列表 24/24

2/3 第一页 上一页 下一页 最后页 前往 第 页 搜索

目的地址	网关地址	接口号	路由状态	优先级	跳数	使用次数	使用时间
192.168.123.1/32	10.10.10.12	ptp1	lughN	60	1	0	633
192.168.16.0/24	-	ie0	cua	20	0	8980	19983
192.168.16.1/32	-	local	cuhp	20	0	6564	19983
200.200.200.0/24	-	ie1	cuaN	20	0	15	2145
200.200.200.1/32	-	local	cuhp	20	0	3605	2145
200.200.200.102/32	-	local	cuhp	20	0	1227	427308
211.200.200.131/32	200.200.200.173	ie1	lughpaN	60	1	20	13
224.0.0.0/4	-	mcast	cup	20	0	0	427310
224.0.0.18/32	-	bhole0	cuhp	20	0	0	427310
224.0.0.5/32	-	bhole0	cuhp	20	0	0	427310

表 5-17 路由表信息列表（续表 5-16）

当 PPTP/L2TP 隧道连接中断后，在*系统状态—>路由和端口信息*的“路由表信息列表”中，可以查看到上网线路的路由被激活，而此时 HiPER VPN 网关会根据配置来决定是否建立 PPTP/L2TP 隧道连接，如表 5-18 所示。

路由表信息列表 20/20

1/2 第一页 上一页 下一页 最后页 前往 第 页 搜索

目的地址	网关地址	接口号	路由状态	优先级	跳数	使用次数	使用时间
0.0.0.0/0	200.200.200.173	ie1	lugpaN	60	1	0	62
0.0.0.0/0	-	ptpdial0	*luga	119	7	0	62
127.0.0.0/8	-	bhole0	cup	20	0	0	427985
127.0.0.1/32	-	local	cuhp	20	0	0	427985
127.0.0.2/32	-	reject0	cuhp	20	0	0	427985
127.0.0.3/32	-	bhole0	cuhp	20	0	0	427985
192.168.1.1/32	-	local	cuhp	20	0	684	427983
192.168.16.0/24	-	ie0	cua	20	0	11400	20658
192.168.16.1/32	-	local	cuhp	20	0	8208	20658
200.200.200.0/24	-	ie1	cuaN	20	0	25	2820

表 5-18 路由表信息列表

提示：在 PPTP/L2TP 隧道上启用了 NAT，PPTP/L2TP 隧道连通之后，只能实现 PPTP/L2TP 客户端到 PPTP/L2TP 服务器的单向访问，从 PPTP/L2TP 服务器到 PPTP/L2TP 客户端的访问将被拒绝。

5.4.3 缺省网关不是 PPTP/L2TP 服务器的实现方法

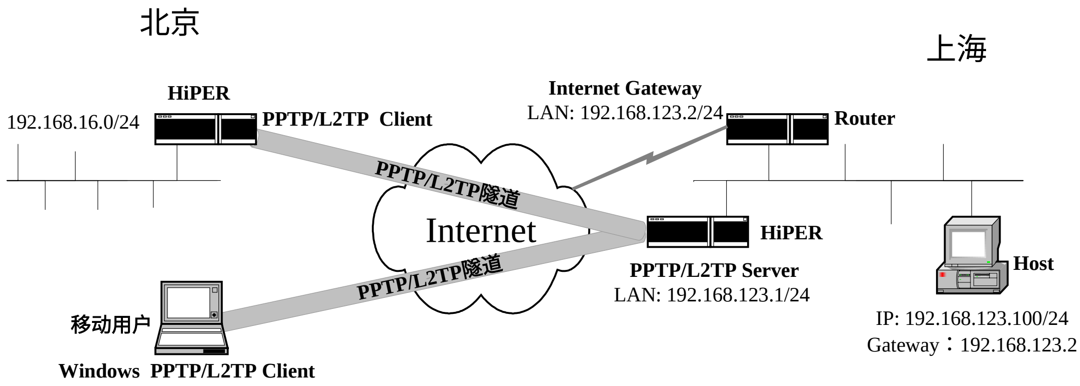


图 5-69 方案——缺省网关不是 PPTP/L2TP 服务器

某些局域网有两台路由器，一台作为上网的网关，一台作为连接 PPTP/L2TP 隧道的路由器。如图 5-69 所示，上海的局域网的每台计算机网关都指向 Internet Gateway，没有指向 PPTP/L2TP 服务器。那么虽然北京或者移动用户能够连接到 PPTP/L2TP 隧道，但是仍然不能通过 PPTP/L2TP 隧道访问上海的计算机。

以下三种方法可以解决以上的问题：

1. 方法一 在上海局域网中的每台计算机中添加静态路由

分别为每台计算机添加一条访问北京局域网（192.168.16.0/24）的路由，和一条访问移动用户的路由（假设 PPTP/L2TP 服务器的地址池是 10.10.10.0/24），可在 DOS 窗口下依次输入：

route add 192.168.16.0 mask 255.255.255.0 192.168.123.1

route add 10.10.10.0 mask 255.255.255.0 192.168.123.1

提示：

按上述方式在计算机上添加的静态路由在计算机重启后需要重新添加，可以采取以下方法解决这个问题：如果是 Windows 2000/XP 的计算机可以使用命令 *route add 192.168.16.0 mask 255.255.255.0 192.168.123.1 –p* 添加永久路由；

2. 方法二 在 Internet Gateway 中添加静态路由

如果 Internet Gateway 是 HiPER VPN 网关，则可以为其设置静态路由。

1) 设置访问北京局域网（192.168.16.0/24）的路由

在***高级配置—>路由配置—>路由参数设置***中，选中 “ 添加 ” 按钮，在相关配置参数项中依次填入以下内容，再单击 “ 保存 ” 按钮，如图 5-70 所示。

“ 路由设置名 ”：route_bj

“ 目的网络 ”：192.168.16.0

“ 网络掩码 ”：255.255.255.0

“ 网关地址 ”：192.168.123.1

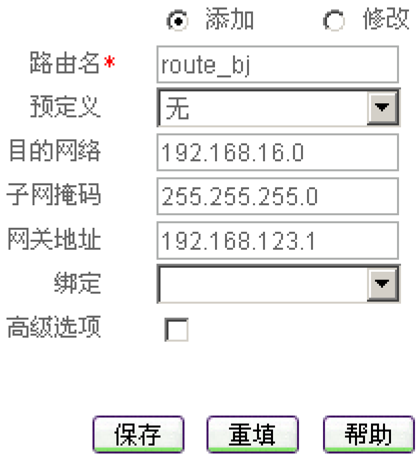


图 5-70 路由参数设置

2) 设置访问移动用户的的路由

这里假设 PPTP/L2TP 服务器的地址池是 10.10.10.0/24。

在***高级配置—>路由配置—>路由参数设置***中，选中 " 添加 " 按钮，在相关配置参数项中依次填入以下内容，再单击 " 保存 " 按钮，如图 5-71 所示。

" 路由设置名 "：route_mobil

" 目的网络 "：10.10.10.0

" 网络掩码 "：255.255.255.0

" 网关地址 "：192.168.123.1



图 5-71 路由参数设置

提示：如果 Internet Gateway 是其他品牌路由器，会有类似的设置静态路由的界面。

3. 方法三 在 PPTP/L2TP 服务器上启用 ARP 代理

1) 设置 PPTP/L2TP 服务器地址池相关参数

在 ***VPN 配置—>PPTP 和 L2TP*** 中，如图 5-72 所示，在 " 地址池开始地址 " 和 " 地址池地址数 " 中分别填入 " 192.168.123.220 "、" 20 "，这个地址池为 PPTP/L2TP 服务器端一段空闲的局域网 IP 地址（原要求地址池不能设置成任何 VPN 网段的 IP 地址段）；

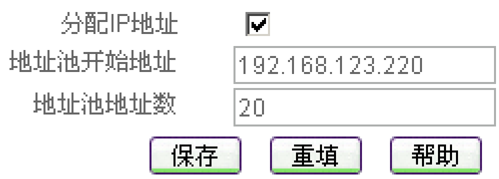


图 5-72 路由参数设置

2) 在 HiPER 的 LAN 口启用 ARP 代理

进入***基本配置—>接口配置***页面中，如图 5-73 所示，首先在“ 选择接口 ”选择“ LAN ”，在“ ARP 代理 ”中选择“ Enabled ”，再单击“ 保存 ”按钮。



图 5-73 ARP 代理设置

提示：在 PPTP/L2TP 服务器上启用 ARP 代理之后，拨入的 PPTP/L2TP 客户端只能是移动用户。如果想实现一个局域网通过路由器连接到 PPTP/L2TP 服务器，就必须在 PPTP/L2TP 隧道上启用 NAT，可以参考章节 5.4.1 里面的设置，但是这样只能是实现 PPTP/L2TP 客户端局域网到 PPTP/L2TP 服务器端局域网的单向访问。

5.4.4 PPTP/L2TP 服务器端的局域网用户访问移动用户的方法

当有移动用户通过 PPTP/L2TP 隧道连接到 PPTP/L2TP 服务器时，PPTP/L2TP 服务器会从其地址池分配一个 IP 地址给移动用户，移动用户可以使用这个分配的 IP 地址访问 PPTP/L2TP 服务器端的局域网，PPTP/L2TP 服务器端的局域网用户也可以通过访问这个分配的 IP 地址来访问移动用户。在 ***VPN 配置—>PPTP 和 L2TP*** 中，查看“ PPTP/L2TP 信息列表 ”，可以查到分配的 IP 地址（10.10.10.18），如表 5-19、表 5-20 所示（这里以 HiPER 作为 PPTP 服务器为例进行说明）。

PPTP/L2TP 信息列表 2/6

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

	设置名	用户名	允许	会话状态	远端网关	远端内网地址	使用时间
☐	vpn_mobile	vpn_mobile	☑	已连接	192.168.123.13	192.168.210.34	00:00:00:0
☐	vpn_bj	vpn_bj	☑	已连接	211.200.200.1	192.168.16.0	00:00:31:2

表 5-19 HiPER 作为 PPTP 服务器—PPTP/L2TP 信息列表

PPTP/L2TP 信息列表 2/6

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

	使用时间	空闲时间	出流量	入流量	业务类型	协议类型	虚接口地址	是否加密
	00:00:00:07	00:00:00:02	437	1782	VPN拨入	PPTP	10.10.10.16	否
	00:00:31:24	00:00:31:24	38619	4834	VPN拨入	PPTP	10.10.10.17	否

表 5-20 HiPER 作为 PPTP 服务器—PPTP/L2TP 信息里表（续表 5-19）

由于每次移动用户通过 PPTP/L2TP 隧道连接到 PPTP/L2TP 服务器时，都有可能被分配到不同的 IP 地址，因而每次 PPTP/L2TP 服务器端的局域网用户访问移动用户时，都要到 ***VPN 配置—>PPTP 和 L2TP*** 页面查看" PPTP/L2TP 信息列表 "，查询当前分配给移动用户的 IP 地址。为了避免这个麻烦，可以在移动用户计算机上设定固定的 IP 地址。方法如下（这里以 Windows XP 为例说明）：

双击已经在移动用户计算机上设置好的 PPTP/L2TP 隧道连接名，单击" 属性 "，在" 网络 " 属性页面，双击" Internet 协议（TCP/IP）属性 "，如图 5-74 所示，选中" 使用下面的 IP 地址 "，填入" 10.10.10.90 "（PPTP/L2TP 服务器地址池以外的 IP 地址），那么每次移动用户通过 PPTP/L2TP 隧道连接到 PPTP/L2TP 服务器后，PPTP/L2TP 服务器端的局域网用户都可以使用 10.10.10.90 这个 IP 地址来访问移动用户。

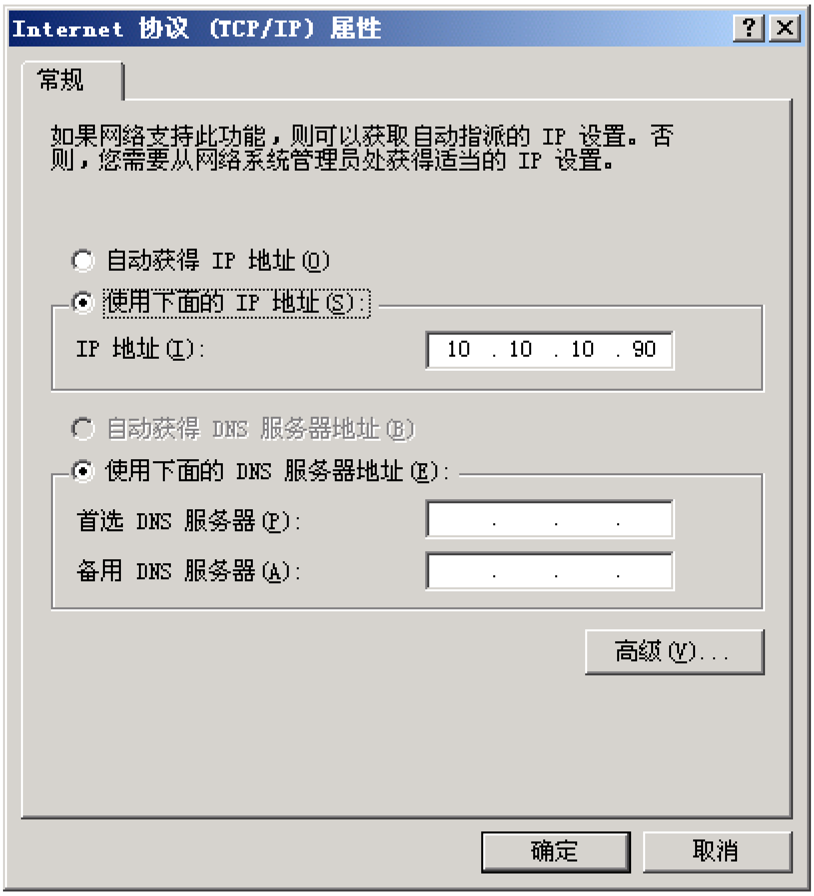


图 5-74 Internet 协议（TCP/IP）属性界面

5.4.5 解决 Windows 移动用户连接 VPN 隧道成功后默认路由被修改的方法

移动用户在建立 PPTP/L2TP 隧道连接之前，在 DOS 窗口执行 route print 命令可以看到默认路由如表 5-21 所示：

Active Routes:				
Network Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	200.200.200.254	200.200.200.175	1

表 5-21 路由表一（查看默认路由）

移动用户在 PPTP/L2TP 隧道连接成功之后，在 DOS 窗口执行 route print 命令看到默认路由如表 5-15 所示：

Active Routes:				
Network Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	10.10.10.16	10.10.10.16	1
0.0.0.0	0.0.0.0	200.200.200.254	200.200.200.175	2

表 5-22 路由表二（查看默认路由）

此时，默认路由被指向 PPTP/L2TP 服务器，这就意味着移动用户所有的上网请求（到 PPTP/L2TP 服务器端的局域网和其他网络）都将被转发到 PPTP/L2TP 服务器上，这样就会造成移动用户无法上网或者是 PPTP/L2TP 服务器端上网带宽的的浪费。

解决方法是（这里以 Windows XP 为例说明）：

1. 双击在移动用户计算机上已经设置好的 PPTP/L2TP 隧道连接名，单击“属性”，在“网络”属性页面，双击“Internet 协议（TCP/IP）属性”，选中“使用下面的 IP 地址”，填入“10.10.10.90”（PPTP/L2TP 服务器地址池以外的 IP 地址）。
2. 单击“高级”，取消“在远程网络上使用默认网关”的选中，单击两次“确定”。
3. 单击“连接”，发起建立 PPTP/L2TP 隧道请求。
4. PPTP/L2TP 隧道连接成功后，在 DOS 窗口执行添加路由命令：

   route add 192.168.123.0 mask 255.255.255.0 10.10.10.90

此时，在 DOS 窗口执行 route print 命令可以看到上网的路由没有改变，而到 PPTP/L2TP 服务器端的局域网的请求将被转发到 PPTP/L2TP 隧道，如表 5-23 所示。

Active Routes:				
Network Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	200.200.200.254	200.200.200.175	1
192.168.123.0	255.255.255.0	10.10.10.90	10.10.10.90	1

表 5-23 路由表三（查看默认路由）

提示：

为了避免每次重启后在移动用户中添加路由的麻烦，可以将静态路由存成一个*.bat 文件，在 PPTP/L2TP 隧道连接成功后执行一下即可。

5.4.6 多分支 PPTP/L2TP 隧道互联（配置远端内网 IP 地址方式）

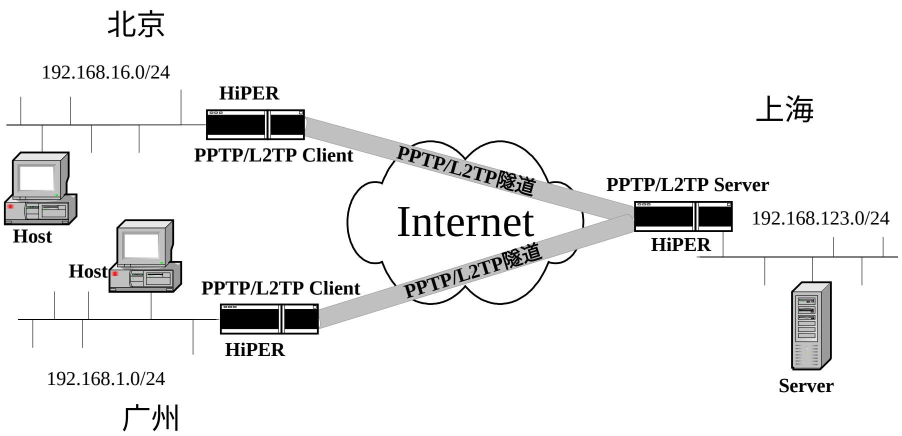


图 5-75 方案——多分支 PPTP/L2TP 隧道互联（一）

如图 5-75 所示，某公司的本部在上海，在北京和广州分别设有分公司。通过在上海使用 HiPER VPN 网关作为 PPTP/L2TP 服务器，在北京和广州分别使用 HiPER VPN 网关作为 PPTP/L2TP 客户端，同时在北京和上海、广州和上海之间建立 PPTP/L2TP 隧道。

其中，PPTP/L2TP 客户端（北京）的局域网网段是 192.168.16.0/255.255.255.0，PPTP/L2TP 客户端（广州）的局域网网段是 192.168.1.0/255.255.255.0，PPTP/L2TP 服务器端（上海）的局域网网段是 192.168.123.0/255.255.255.0。

常规配置方式下，在北京和上海、广州和上海的 PPTP/L2TP 隧道连接成功之后，只能实现北京和上海、广州和上海的互访，而不能实现广州和北京的互访。可以通过调整北京和广州的 HiPER VPN 网关的“远端内网 IP 地址”、“远端内网子网掩码”的方式解决这个问题。

由于北京、广州、上海三地的局域网网段都属于 192.168.0.0/255.255.0.0 这个大网段，因而就可以在北京、广州的 HiPER VPN 网关中，将“远端内网 IP 地址”、“远端内网子网掩码”作如下设置（此处以北京的 HiPER VPN 网关为例）：

在 ***VPN 配置—>PPTP 和 L2TP*** 中，将“远端内网 IP 地址”配置成“192.168.0.0”、“远端内网子网掩码”配置成“255.255.0.0”。

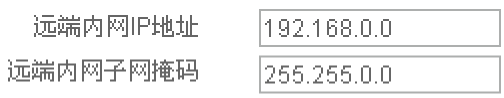


图 5-76 PPTP/L2TP 隧道参数（远端内网 IP 地址）设置

北京的 HiPER VPN 网关和 PPTP/L2TP 服务器连接成功之后，在***系统状态—>路由和端口信息***的“路由表信息列表”中可以看到目的地址为 192.168.0.0/16 路由，如表 5-24 所示，这表示局域网中到上海（192.168.123.0/255.255.255.0）或者广州（192.168.1.0/255.255.255.0）的访问数据都会通过 PPTP/L2TP 隧道转发。

目的地址	网关地址	接口号	路由状态	优先级	跳数	使用次数	使用时间
0.0.0.0/0	200.200.200.173	ie1	lugpaN	60	1	0	9
10.10.10.17/32	-	local	Ruhtp	60	0	0	9
127.0.0.0/8	-	bhole0	cup	20	0	0	432054
127.0.0.1/32	-	local	cuhp	20	0	0	432054
127.0.0.2/32	-	reject0	cuhp	20	0	0	432054
127.0.0.3/32	-	bhole0	cuhp	20	0	0	432054
192.168.0.0/16	10.10.10.17	ptp3	lug	60	1	0	9
192.168.0.0/32	10.10.10.17	ptp3	lugh	60	1	0	9

表 5-24 路由表信息列表

广州的 HiPER VPN 网关作同样的配置。这样，当北京和上海、广州和上海之间的 PPTP/L2TP 隧道均连接成功之后，北京和广州的局域网用户就可以通过 PPTP/L2TP 隧道（在上海中转）进行相互访问，上海、北京和广州之间就实现了多分支 PPTP/L2TP 隧道互联。

提示：

不需要调整 PPTP/L2TP 服务器端的 HiPER VPN 网关中原先已配置的“远端内网 IP 地址”、“远端内网子网掩码”参数。

5.4.7 多分支 PPTP/L2TP 隧道互联（手工添加静态路由方式）

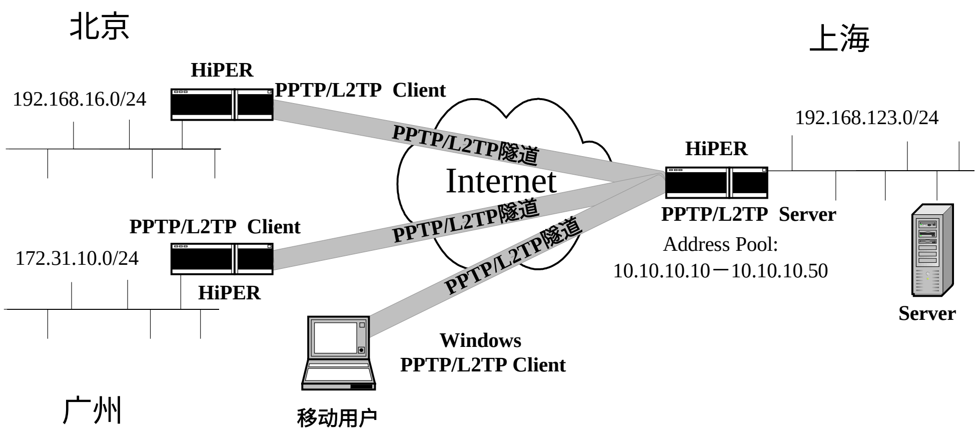


图 5-77 方案——多分支 PPTP/L2TP 隧道互联（二）

在 5.4.6 节的实例中，北京、上海、广州三地的局域网都处在同一个大网段中，但是如果它们不是处于同一个大网段中，则无法通过配置远端内网 IP 地址的方法实现多分支 PPTP/L2TP 隧道，但是可以通过使用配置静态路由的方法来解决这个问题。

如图 5-77 所示，本实例背景同 5.4.6 节的实例，所不同的是各端局域网不再处于同一大网段中，其中：PPTP/L2TP 客户端（北京）的局域网网段是 192.168.16.0/255.255.255.0，PPTP/L2TP 客户端（广州）的局域网网段是 172.31.10.0/255.255.255.0，PPTP/L2TP 服务器端（上海）的局域网网段是 192.168.123.0/255.255.255.0。另外，在本例中，还增加了移动用户作为 PPTP/L2TP 客户端，其网段是 10.10.10.0/255.255.255.255（由于在本例中，为 PPTP/L2TP 服务器配置的“地址池”是 10.10.10.10~10.10.10.50）。

要实现北京、广州和移动用户之间通过 PPTP/L2TP 隧道互联，配置方法如下（以北京的 HiPER VPN 网关为例）：

1. 配置到上海的 PPTP/L2TP 隧道的相关参数

在 ***VPN 配置—>PPTP 和 L2TP*** 中，选中“添加”选项，将“设置名”设置为“VPN_remote”、“远端内网 IP 地址”设置为“192.168.123.1”、“远端内网子网掩码”设置为“255.255.255.0”，如图 5-78 所示。



图 5-78 VPN 隧道参数设置

2. 配置到广州的静态路由

在***高级配置—>路由配置***的“路由参数设置”中，选中“添加”选项，将“路由名”设置为“vpn_gz”、“目的网络”设置为“172.31.10.0”、“网络掩码”设置为“255.255.255.0”、“绑定”在 “VPN_remote”（第 1 步配置 PPTP/L2TP 隧道时填写的“设置名”），如图 5-79 所示。



图 5-79 路由参数设置

3. 配置到移动用户的静态路由

在***高级配置—>路由配置***的“路由参数设置”中，选中“添加”按钮，将“路由名”设置为“vpn_mobile”、“目的网络”设置为“10.10.10.0”、“网络掩码”设置为“255.255.255.0”，“绑定”在 “VPN_remote”（第 1 步配置 PPTP/L2TP 隧道时填写的“设置名”），如图 5-80 所示。



图 5-80 路由参数设置

北京的 HiPER VPN 网关和 PPTP/L2TP 服务器连接成功之后，在*系统状态—>路由和端口信息*的“路由表信息列表”中可以看到有到上海、广州、移动用户的路由，如表 5-25 所示，这就表示局域网中到上海（192.168.123.0/255.255.255.0）、广州（172.31.10.0/255.255.255.0）和移动用户（10.10.10.0/255.255.255.0）的访问数据都会通过 PPTP/L2TP 隧道转发。

路由表信息列表　23/23

1/3　第一页　上一页　下一页　最后页　前往 第　页　搜索

目的地址	网关地址	接口号	路由状态	优先级	跳数	使用次数	使用时间
0.0.0.0/0	200.200.200.173	ie1	lugpaN	60	1	20	12
10.10.10.0/24	10.10.10.19	ptp4	lugp	60	1	0	12
10.10.10.19/32	-	local	Ruhtp	60	0	0	12
127.0.0.0/8	-	bhole0	cup	20	0	0	433297
127.0.0.1/32	-	local	cuhp	20	0	0	433297
127.0.0.2/32	-	reject0	cuhp	20	0	0	433297
127.0.0.3/32	-	bhole0	cuhp	20	0	0	433297
172.31.10.0/24	10.10.10.19	ptp4	lugp	60	1	0	12
192.168.123.0/24	10.10.10.19	ptp4	lug	60	1	0	12
192.168.123.1/32	10.10.10.19	ptp4	lugh	60	1	0	12

表 5-25 路由表信息列表

广州的 HiPER VPN 网关作同样的配置。这样，当北京和上海、广州和上海、移动用户和上海之间的 PPTP/L2TP 隧道均连接成功之后，北京和广州的局域网用户以及移动用户就可以通过 PPTP/L2TP 隧道（在上海中转）进行相互访问，上海、北京、广州以及移动用户之间就实现了多分支 PPTP/L2TP 隧道互联。

提示：

1. 不需要调整 PPTP/L2TP 服务器端的原先设置的参数“远端内网 IP 地址”和“远端内网子网掩码”。
2. 如果移动用户按照章节 5.4.5 的方式配置了计算机，那么在这个方案中移动用户还要添加到北京、广州的静态路由。

    route add 192.168.16.0 mask 255.255.255.0 10.10.10.90

    route add 172.31.10.0 mask 255.255.255.0 10.10.10.90

5.5 备注

本章涉及到的其他厂商的产品型号以及软件版本如表 5-26 所示：

型号	版本
Windows 2000 Server	Microsoft windows 2000 5.00.2195 Service Pack 4
Windows XP	Microsoft windows XP Professional 版本 2002 Service Pack 2
Cisco 3600	c3620-ik9o3s7-mz.123-3a.bin
FortiGate-60/300A	Fortigate-60 2.50,build251,040422
NetScreen208	Version: 4.0.1r6.0（Firewall+VPN）

表 5-26 其他厂商产品型号及软件版本

第6章 HiPER IPSec 配置

6.1 IPSec 配置界面

IPSec 隧道存在于两个网关之间，每个网关需要一个 IP 地址。正如前所述（章节 4.2.1.2），IPSec 的密钥管理对 IPSecVPN 的使用很关键，IPSec 支持手动和自动密钥分配方法。手动密钥方式应用于较小和简单的网络，安全性较弱，而且它要求两个网关都使用固定 IP 地址；自动密钥方式大量应用于实际网络，它不仅可以应用于隧道两端网关均使用固定地址的情况，还可以应用于其中一个网关是动态地址的情况。另外，HiPER VPN 网关支持动态 DNS，可以将变化的 IP 地址映射到固定的域名，因此，如果使用 HiPER，还可以在两个地址都不固定的情况下建立 IPSec 隧道。

HiPER VPN 网关中，有以下几种配置 IPSec 隧道的方式（详见章节 4.2）：

1. “手动”方式，网关到网关，使用手动密钥交换；
2. “自动”方式，网关到网关，使用自动 IKE，主模式；
3. “自动”方式，动态连接到网关，使用自动 IKE，野蛮模式；
4. “自动”方式，对方动态连接到本地，使用自动 IKE，野蛮模式。

第 3 种情况 HiPER 是通过动态分配得到地址，而隧道对等方网关具有一个固定地址，因为 HiPER 的地址不固定，所以隧道的发起方是 HiPER，发起方必须提供身份，如以 Email 的形式等；第 4 种情况是 HiPER 具有固定 IP 地址，而隧道对等方网关拥有动态地址，同样，隧道的发起方是 HiPER 的对等方，它也必须提供身份认证。

最后，当在动态对等方和固定对等方之间建立好隧道之后，如果目的主机有固定的 IP 地址，在两个网关之中的任一个网关后面的主机，均可通过隧道发送数据。

6.1.1 IPSec 的配置参数

在 IPSec 页面，通过将“设置方式”选择为“手动”实现手动配置 IPSec 隧道，如图 6-1 所示；通过将“设置方式”选择为“自动”实现自动配置 IPSec 隧道，如图 6-3 所示。

1. 手动方式

手动方式只允许配置网关到网关的隧道。

1) **基本参数配置**



图 6-1 IPSec 配置界面（手动方式）

- 设置名：IPSec 隧道的名称（自定义，不可重复，不能超过 10 个字符）；
- 设置方式：手动，通过手动协商方式建立 IPSec 隧道；
- 远端网关地址（名）：IPSec 隧道远端网关的地址（或域名），设置为域名时，需要在 HiPER 上设置 DNS 服务器，此时 HiPER 会定期解析该域名，如果 IP 地址发生了变化，HiPER 将重新协商 IPSec 隧道；
- 远端内网地址：IPSec 隧道远端受保护的内网的任一 IP 地址，如果远端是移动单机用户，则填写该设备的 IP 地址；
- 远端内网掩码：IPSec 隧道远端受保护的内网的子网掩码，如果远端是移动单机用户，则填写 255.255.255.255；

- 本地绑定：选择本地接口的类型，接口可以是以太网口，或 PPPoE 拨号连接，还可以是 PPTP/L2TP 拨号连接；如果将 IPSec 隧道配置为绑定到该接口上，那么所有经过该接口的数据包将通过 IPSec 检查，以确定是否对该数据包进行加密和解密操作；
- 本地内网地址：本地受保护的内网的任一 IP 地址；
- 本地内网掩码：本地受保护的内网的子网掩码；
- ESP 加密算法：使用 ESP 协议加密时使用的算法，有“DES”、“3DES”、“AES128”、“AES192”、“AES256”、“NONE”六个选项；
- ESP 加密密钥：ESP 协议加密时使用的密钥，DES 需要 8 个字节，3DES 需要 24 个字节，AES128 需要 16 个字节，AES192 需要 24 字节，AES256 需要 32 字节。在本项中输入的是加密字符串所对应的十六进制的 ASCII 码，每两个字符的组合表示十六进制格式中的一个字节。如加密密钥为“1K3PM678”，那么需要输入“314B33504D363738”；
- ESP 认证算法：ESP 协议认证时使用的算法，选项有“MD5”、“SHA”及“NONE”；
- ESP 认证密钥：ESP 协议认证时使用的密钥，MD5 需要 16 字节，SHA-需要 20 字节，输入方式同 ESP 加密密钥。
- AH 认证算法：ESP 协议加密时使用的算法，选项有“MD5”、“SHA”及“NONE”；
- AH 认证密钥：AH 协议认证时使用的密钥；MD5 需要 16 字节，SHA 需要 20 字节，输入方式同 ESP 加密密钥。
- ESP 外出 SPI：该隧道使用 ESP 时，外出的 SPI；
- ESP 进入 SPI：该隧道使用 ESP 时，进入的 SPI；
- AH 外出 SPI：该隧道使用 AH 时，外出的 SPI；
- AH 进入 SPI：该隧道使用 AH 时，进入的 SPI；
- 保存：IPSec 配置参数检查并提交；
- 重填：恢复旧的配置参数数据；
- 帮助：打开 IPSec 帮助页面。

提示：

1. 常用字符的十六进制 ASCII 码表见附录一；
2. 在“ESP 外出 SPI”、“ESP 进入 SPI”、“AH 外出 SPI”、“AH 进入 SPI”这几个参数中均需填入十进制数字，最小值是 256，最大值是 4,294,967,295（0xFFFF FFFF）。本端外出的 SPI 和对端进入的 SPI 值必须相等；本端进入的 SPI 和对端外出的 SPI 值也必须相等。

2) 高级选项配置



图 6-2 IPSec 配置界面（手动方式）——高级选项

- 高级选项：选中后显示 IPSec 隧道的高级配置参数；
- 协议：需要进行 IPSec 保护的数据包的协议类型，有“任意”、“TCP”、“UDP”、“ICMP”四个选项；
- 端口：需要进行 IPSec 保护的数据包的端口号，“0”表示任意端口。注意，“协议”为“任意”时，端口配置无效，因此，如果需要配置“端口”，必须选择“协议”（TCP

或 UDP）；

- 抗重播：启用或取消抗重播功能；选中后，HiPER VPN 网关将支持抗重播功能，从而可以拒绝接收过的数据包或数据包拷贝，以保护自己不被攻击。

2. 自动方式

自动方式下有“网关到网关”，“动态连接到网关”和“对方动态连接到本地”三种配置方式可选。每个页面配置包括基本参数配置和高级选项配置，以上三种方式的高级选项配置页面一样，下面先介绍三种方式的基本参数配置，然后统一介绍高级选项配置。

1) 基本参数配置

a) 网关到网关

网关到网关（如图 6-3 所示）也就是 LAN 到 LAN 的 IPSec VPN 方式，通信双方地址固定，本方式不要配置身份 ID。



图 6-3 IPSec 配置界面（自动方式——网关到网关）

- 设置名：IPSec 隧道的名称（自定义，不可重复，不超过十个字符）；
- 设置方式：自动，通过自动协商方式建立 IPSec 隧道；
- 自动方式：网关到网关；
- 远端网关地址（名）：IPSec 隧道远端网关的地址（或域名），设置为域名时，需要

在 HiPER 上设置 DNS 服务器，此时 HiPER 会定期解析该域名，如果 IP 地址发生变化，HiPER 将重新协商 IPSec 隧道；

- 远端内网地址：IPSec 隧道远端受保护的内网的任一 IP 地址，如果远端是移动单机用户，则填写该设备的 IP 地址；
- 远端内网掩码：IPSec 隧道远端受保护的内网的子网掩码，如果远端是移动单机用户，则填写 255.255.255.255；
- 本地绑定：选择本地接口的类型，接口可以是以太网口，或 PPPoE 拨号连接，还可以是 PPTP/L2TP 拨号连接；如果将 IPSec 隧道配置为绑定到该接口上，那么所有经过该接口的数据包将通过 IPSec 检查，以确定是否对该数据包进行加密和解密操作；
- 本地内网地址：本地受保护的内网的任一 IP 地址；
- 本地内网掩码：本地受保护内网的子网掩码；
- 预共享密钥：协商所用的预共享密钥，最长为 128 个字符；
- 加密认证算法 1：可供第二阶段协商使用的首选加密认证算法。

b) 动态连接到网关

动态连接到网关（如图 6-4 所示）指 HiPER VPN 网关作为 IPSec 隧道的发起方，本方式下，HiPER 的地址不固定，必须采用野蛮模式进行协商。



图 6-4 IPSec 配置界面（自动方式——动态连接到网关）

本方式中，配置参数 “ 远端网关地址 ”、“ 远端内网地址 ”、“ 远端内网掩码 ”、“ 本地绑

定”、“本地内网地址”、“本地内网掩码”、“预共享密钥”以及“加密认证算法 1”的含义与“网关到网关”自动方式中的对应参数含义相同，这里不再重复描述，请参照“网关到网关”方式中的相关解释。

不同之处在于，本方式中需要进行身份认证，相关参数解释如下：

- 远端身份 ID：用来认证远端的身份 ID（可选）；
- 远端身份类型：远端身份 ID 的类型，有 “Email 地址”、“特殊字节流”、“域名”及“IP 地址”四个选项；
- 本地身份 ID：本地发送给远端认证的身份 ID，必须设置；
- 本地身份类型：本地身份 ID 的类型，有“Email 地址”、“特殊字节流”、“域名”及“IP 地址”四个选项，必须设置。

c) 对方动态连接到本地

对方动态连接到本地（如图 6-5 所示）指 HiPER 作为 IPSec 隧道的响应方，本方式下，对方地址不固定。



图 6-5 IPSec 配置界面（自动方式——对方动态连接到本地）

本方式中，配置参数 “远端网关地址”、“远端内网地址”、“远端内网掩码”、“本地绑定”、“本地内网地址”、“本地内网掩码”、“预共享密钥”以及“加密认证算法 1”的含义与

“网关到网关”自动方式中的对应参数含义相同，这里不再重复描述，请参照“网关到网关”方式中的相关解释。

不同之处在于，本方式中需要进行身份认证，相关参数解释如下：

- 远端身份 ID：用来认证远端的身份 ID，必须设置；
- 远端身份类型：远端身份 ID 的类型，有“Email 地址”、“特殊字节流”、“域名”及“IP 地址”四个选项，必须设置；
- 本地身份 ID：本地发送给远端认证的身份 ID（可选）；不设定时，不主动发送本地身份供远端认证；
- 本地身份类型：本地身份 ID 的类型，本地身份 ID 的类型，有“Email 地址”、“特殊字节流”、“域名”及“IP 地址”四个选项。

2) **高级选项配置**

以上三种自动方式的高级选项配置界面基本相同，其中：“网关到网关”方式下，“协商模式”选择为“主模式”（如图 6-6）；另外两种方式下，“协商模式”选择为“野蛮模式”（如图 6-7）。由于野蛮模式和主模式相比，除了多出“野蛮模式加密协商”这个选项，其他配置参数完全相同，故在这里以野蛮模式下的高级选项配置为例进行说明，主模式的配置参数含义参照野蛮模式。



图 6-6 IPSec 配置界面（自动方式）——高级选项（主模式）



图 6-7 IPSec 配置界面（自动方式）——高级选项（野蛮模式）

- 协议：需要进行 IPSec 保护的数据包的协议类型，有“ 任意 ”、“ TCP ”、“ UDP ” 及 “ ICMP ” 四个选项；
- 端口：需要进行 IPSec 保护的数据包的端口号，“ 0 ” 表示任意端口。注意，“ 协议 ” 为“ 任意 ”时，端口配置无效，因此，如果需要配置“ 端口 ”，必须选择“ 协议 ”（TCP 或 UDP）；
- 协商模式（第一阶段）：“ 主模式 ”或“ 野蛮模式 ”，“ 网关到网关 ”时选择“ 主模式 ”，其他两种方式时选择 “ 野蛮模式 ”；
- 野蛮模式协商加密：指野蛮模式下，第二个信息包是否加密。HiPER 作为响应方时，支持加密和不加密两种方式；
- 生存时间（第一阶段）：IKE SA 的生存时间，至少 600 秒，当剩余时间为 540 秒时，将重新协商 IKE SA；
- 加密认证算法 1—加密认证算法 4（第一阶段）：第一阶段协商使用的加密认证算法，可以选择四组，每组为不同的加密算法、认证算法及 DH 组的组合；
- 加密认证算法 2—加密认证算法 4（第二阶段）：第二阶段协商使用的加密认证算法，

可选三组，加上在基本参数配置中已配置的一组，共四组；

- 生存时间（第二阶段）：IPSec SA 的生存时间，至少 600 秒，当剩余时间为 540 秒时，SA 将过期，重新协商 IPSec SA；
- 最大流量：每次 IPSec 会话允许通过的最大流量（单位：千字节数），超过后，SA 将重新协商；
- 抗重播：启用或取消抗重播功能；
- DPD：启用或取消 DPD 功能；
- 心跳：在这里配置时间间隔，单位为秒。配置该值后，HiPER VPN 网关会每隔单位时间（“心跳”）向对端发送探测消息，来确定对端是否还存活。
- NAT 穿透：启用或取消 NAT 穿透功能；
- 端口：用来穿透 NAT 的 UDP 封包的端口号，缺省值 4500；
- 维持：启用 NAT 功能后，HiPER 将每隔单位时间（“维持”）向 NAT 设备发送一个数据包以维持 NAT 映射，这样就不需要更改 NAT 映射，直到第一阶段和第二阶段的 SA 过期。

提示：

IPSec 中使用 AH 协议和 ESP 协议保护 IP 层的通信，使用 AH 协议可对数据包进行认证，使用 ESP 协议可对数据包进行加密并认证、仅加密或仅认证。

HiPER VPN 网关中，提供 DES、3DES、AES（包括 AES128、AES192、AES256）这五种加密算法，同时提供 MD5、SHA 这两种认证算法。

第一阶段还支持 DH 交换，提供 DH1、DH2 和 DH5 这三个 DH 组。

第一阶段的加密算法的结构为“加密算法＋认证算法＋DH 组”，由于在第一阶段中，每组加密认证算法均包含上述结构中的三项，故共有 5×3×2＝30 种组合。例如，如果选择“3des-md5-group2”即表示选择的加密算法为 3DES、认证算法为 MD5、DH 组为 DH2。

WEB UI 方式下，由于系统提供 4 组缺省的第一阶段加密认证算法以供选择，故某些情况下，无需配置第一阶段的加密认证算法；另外，每次最多可以配置 4 组第一阶段加密认证算法（CLI 方式下最多可提供 12 组），以供选择。

第二阶段的加密算法的结构为“加密算法（使用 ESP）＋认证算法（使用 ESP）＋认证算法（使用 AH）”，由于在第二阶段中，每组加密认证算法可以包含上述结构中的三项，也可以仅包含一项或两项（至少一项），故共有 6×3×3－1＝53 种组合。具体组合形式如下：

1. 使用 ESP 加密（5 种）
   例如，如果选择“esp-des”，即表示使用 ESP 加密（算法为 DES）；
2. 使用 ESP 认证（2 种）
   例如，如果选择“esp-md5”，即表示使用 ESP 认证（算法为 MD5）；
3. 使用 AH 认证（2 种）
   例如，如果选择“ah-sha”，即表示使用 AH 认证（算法为 SHA）；
4. 使用 ESP 加密和 ESP 认证（5×2＝10 种）
   例如，如果选择“esp-aes128-sha”，即表示使用 ESP 加密和认证（算法分别为 AES128、SHA）；
5. 使用 ESP 加密和 AH 认证（5×2＝10 种）
   例如，如果选择“esp-aes192-ah-md5”，即表示使用 ESP 加密（算法为 AES192），同时使用 AH 认证（算法为 MD5）；
6. 使用 ESP 认证和 AH 认证（2×2＝4 种）
   例如，如果选择“esp-md5-ah-sha”，即表示使用 ESP 认证（算法为 MD5），同时使用 AH 认证（算法为 SHA）；

7. 使用 ESP 加密、ESP 认证和 AH 认证（5×2×2＝20 种）
   例如，如果选择“ esp-aes256-sha-ah-md5 ”，即表示使用 ESP 加密和认证（算法分别为 AES256、SHA），同时使用 AH 认证（算法为 MD5）。

WEB UI 方式下，系统提供 1 组缺省的第二阶段加密认证算法（即“ 安全选项 ”中配置的“ 加密认证算法 1 ”）；另外，最多可以配置 4 组第二阶段的加密认证算法（包括在“ 安全选项 ”中配置的“ 加密认证算法 1 ”）（CLI 方式下最多可提供 12 组），以供选择。

6.1.2 IPSec 信息列表



	设置名	设置方式	允许	SA状态	远端网关	远端内网地址	外出加密包个数	进入解密包个数	本地绑定	本
☐	sh_bj	自动	☑	已建立	135.252.52.240	192.168.2.1	10480	10480	eth2	

表 6-1 IPSec 信息列表



本地内网地址	协商模式	加密认证算法	ESP外出SPI	ESP进入SPI	A
192.168.1.1	主模式	esp-aes256-md5-ah-sha	0x22c4e319(583328537)	0x2d8521e8(763699688)	0x22c4e

表 6-2 IPSec 信息列表（续表 6-1）



入SPI	AH外出SPI	AH进入SPI	生存时间(剩余)	筛选协议	筛选端口	UDP封装
(763699688)	0x22c4e318(583328536)	0x2d8521e7(763699687)	00:00:59:02	0	0	

表 6-3 IPSec 信息列表（续表 6-2）

一旦 IPSec 隧道配置完成提交以后，即可在 IPSec 配置页面的“ IPSec 信息列表 ”（如表 6-1、表 6-2、表 6-3 所示）中查看已建立的 IPSec 隧道的配置及状态信息，各参数含义解释如下：

- 设置名：IPSec 隧道的名称；
- 设置方式：IPSec 隧道的设置方式，“ 手动 ” 或 “ 自动 ”；
- SA 状态：SA 建立的状态，共有四种状态，如表 6-4 所示：

状态	描述
未建立	IPSec SA 没有建立
IKE 协商	IKE SA 没有建立，正在进行第一阶段协商
IPSec 协商	IKE SA 已建立，正在进行第二阶段协商
已建立	IPSec SA 已建立

表 6-4 SA 状态

- 远端网关：IPSec 隧道远端网关的地址；
- 远端内网地址：IPSec 隧道远端受保护内网的 IP 地址（配置时填入的值）；
- 外出加密包个数：通过 IPSec 隧道外出的加密数据包的个数；
- 进入解密包个数：通过 IPSec 隧道进入的解密数据包的个数；
- 本地绑定：该隧道的外出和进入绑定的连接，eth2 表示 WAN 口，使用 PPPoE 绑定时显示的是 PPPoE 连接的名称，使用 IPSec over L2TP/PPTP 时显示的是 L2TP/PPTP 隧道的“ 设置名 ”；
- 本地内网地址：本地受保护内网的 IP 地址（配置时填入的值）；
- 协商模式：IKE 协商的模式，有 “ 主模式 ” 和 “ 野蛮模式 ” 两种；
- 加密认证算法：该隧道使用的加密和认证算法，ESP 加密算法有 DES、3DES、AES，ESP 认证算法有 MD5 和 SHA-1，AH 认证算法有 MD5 和 SHA-1；
- ESP 外出 SPI：该隧道使用 ESP 外出的 SPI（安全协议索引），给出十进制和十六进制两种表示方式；
- ESP 进入 SPI：该隧道使用 ESP 进入的 SPI，给出十进制和十六进制两种表示方式；
- AH 外出 SPI：该隧道使用 AH 外出的 SPI，给出十进制和十六进制两种表示方式；
- AH 进入 SPI：该隧道使用 AH 进入的 SPI，给出十进制和十六进制两种表示方式；
- 生存时间（剩余）：SA 在过期之前的生存时间，当剩余时间为 540 秒时，IPSec 遂道将重新协商 SA；手动方式下，显示为“ 永久 ”，表示该 SA 一直有效（单位：天:时:分:秒）；
- 筛选协议：需要进行 IPSec 加密的协议类型，“ 0 ” 表示任意协议；
- 筛选端口：需要进行 IPSec 加密的协议端口，“ 0 ” 表示任意端口；

- 建立：“ 自动 ”方式下，只有通过流量或手工触发，才能建立 IPSec 隧道的连接；“ 手动 ” 方式下，只有通过手工触发，才能建立 IPSec 隧道的连接。如果选中 “ 设置名 ” 前面的单选框，单击 “ 建立 ” 按钮，就可以通过手动的方式建立该条 IPSec 隧道的连接；
- 挂断：选中 “ 设置名 ” 前面的单选框，单击 “ 挂断 ” 按钮，可以通过手动的方式挂断该条 IPSec 隧道的连接；
- 刷新：单击 “ 刷新 ”，可以显示最新的 “ IPSec 信息列表 ”。

6.1.3 IPSec 隧道的增加、浏览、编辑与删除

- 增加 IPSec 隧道：选中 “ 添加 ” 选项，输入 IPSec 隧道信息，单击 “ 保存 ” 按钮，生成新的 IPSec 隧道，如图 6-1、图 6-3、图 6-4 及图 6-5 所示；

- 浏览 IPSec 隧道：如果已经生成了 IPSec 隧道，可以在“IPSec 信息列表”中查看相关信息及状态，如表 6-1 到表 6-3 所示；
- 编辑 IPSec 隧道：如果想编辑某一 IPSec 隧道，首先点击该 IPSec 隧道的“设置名”超链接，该 IPSec 隧道的信息将填充到相应的编辑框内，然后修改它，再单击“保存”按钮，修改完毕；
- 删除 IPSec 隧道：只需选中 IPSec 隧道（在最左边的方框中打“√”），单击左下角的“删除”按钮，即可删除那些被选中的 IPSec 隧道。

6.2 IPSec 手动配置实例

从章节 6.2 到章节 6.6，我们将给出 HiPER VPN 网关作为 IPSec 隧道网关的典型配置。所有的配置例子均包含了网络拓扑，相关设备的 IP 地址，提供了基于 WEB 页面的配置以及 IPSec 隧道的配置及状态信息。对于非 HiPER 设备，也根据相关情况给出配置及相关信息做参考。

6.2.1 HiPER 和 HiPER 手动方式



图 6-8 方案——HiPER 和 HiPER 手动方式

在本例中，如图 6-8 所示，通过使用以 3DES 加密并经 SHA-1 认证的 ESP，采用“手动”密钥方式在上海和北京办公室之间建立 IPSec 隧道，上海和北京的网关都使用 HiPER VPN 网关。地址如下：

上海的 HiPER：

WAN 口： 218.82.51.172/24

静态网关：218.82.51.1/24

LAN 口： 192.168.1.1/24

北京的 HiPER：

WAN 口： 135.252.52.240/24

静态网关：135.252.52.1/24

LAN 口： 192.168.2.1/24

1. 配置上海的 HiPER VPN 网关

在 ***VPN 配置—>IPSec*** 中，选择“添加”选项，然后在配置参数项中依次输入以下内容（没有列出的参数项无需配置），再单击“保存”按钮。

“设置名”： sh_bj_m

“ 设置方式 ”：手动
“ 远端网关地址(名) ”：135.252.52.240
“ 远端内网地址 ”：192.168.2.0
“ 远端内网掩码 ”：255.255.255.0
“ 本地绑定 ”：WAN1（eth2）
“ 本地内网地址 ”：192.168.1.0
“ 本地内网掩码 ”：255.255.255.0
“ ESP 加密算法 ”：3DES
“ ESP 加密密钥 ”：1234567890abcdef1234567890abcdef1234567890abcdef
“ ESP 认证算法 ”：SHA
“ ESP 认证密钥 ”：1234567890abcdef1234567890abcdef12345678
“ AH 认证算法 ”：NONE
“ ESP 外出 SPI ”：1111
“ ESP 进入 SPI ”：2222

2. 配置北京的 HiPER VPN 网关

在 ***VPN 配置—>IPSec*** 中，选择“ 添加 ”选项，然后在配置参数项中依次输入以下内容（没有列出的参数项无需配置），再单击“ 保存 ”按钮。

“ 设置名 ”：bj_sh_m
“ 设置方式 ”：手动
“ 远端网关地址(名) ”：218.82.51.172
“ 远端内网地址 ”：192.168.1.0
“ 远端内网掩码 ”：255.255.255.0
“ 本地绑定 ”：WAN1（eth2）
“ 本地内网地址 ”：192.168.2.0
“ 本地内网掩码 ”：255.255.255.0
“ ESP 加密算法 ”：3DES
“ ESP 加密密钥 ”：1234567890abcdef1234567890abcdef1234567890abcdef
“ ESP 认证算法 ”：SHA
“ ESP 认证密钥 ”：1234567890abcdef1234567890abcdef12345678
“ AH 认证算法 ”：NONE
“ ESP 外出 SPI ”：2222
“ ESP 进入 SPI ”：1111

3. 查看状态

当双方配置完成，隧道建立连接并开始传输数据后，可以在 ***VPN 配置—>IPSec*** 中，查看“ IPSec 信息列表 ”，得到 IPSec 隧道的相关配置及状态信息，如表 6-5、表 6-6、表 6-7 所示（此处以上海的 HiPER 为例进行说明，北京的 HiPER 类似）。

IPSec 信息列表 1/16

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

	设置名	设置方式	允许	SA状态	远端网关	远端内网地址	外出加密包个数	进入解密包个数
☐	sh_bj_m	手动	☑	已建立	135.252.52.240	192.168.2.0	8030	8030

表 6-5 手动（HiPER 和 HiPER）—IPSec 信息列表

IPSec 信息列表 1/16

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

本地绑定	本地内网地址	协商模式	加密认证算法	ESP外出SPI	ESP进入SPI	AH外出SPI	AH进入SPI
eth2	192.168.1.1		esp-3des-sha	0x457(1111)	0x8ae(2222)		

表 6-6 手动（HiPER 和 HiPER）—IPSec 信息列表（续表 6-5）

IPSec 信息列表 1/16

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

法	ESP外出SPI	ESP进入SPI	AH外出SPI	AH进入SPI	生存时间(剩余)	筛选协议	筛选端口	UDP封装
sha	0x457(1111)	0x8ae(2222)			永久	0	0	

表 6-7 手动（HiPER 和 HiPER）—IPSec 信息列表（续表 6-6）

从表 6-5 中，可以看到“设置方式”显示为“手动”，“SA 状态”显示为“已建立”，“外出加密包个数”和“进入解密包个数”均有数值显示。

从表 6-6 中，可以看到“本地绑定”显示为“eth2”，“加密认证算法”显示为“esp-3des-sha”，“ESP 外出 SPI”显示为“0x457（1111）”，“ESP 进入 SPI”显示为“0x8ae（2222）”。

从表 6-7 中，可以看到“生存时间（剩余）”显示为“永久”，表示该 SA 一直有效。

⌖ 提示：

由于手动密钥方式不检查对方网关的存在和配置，因此，只要在 IPSec 页面上配置正确，查看“IPSec 信息列表”（在 ***VPN 配置—>IPSec*** 中），就能看到 SA 状态显示“已建立”。

6.2.2 HiPER 和 Cisco 路由器手动方式

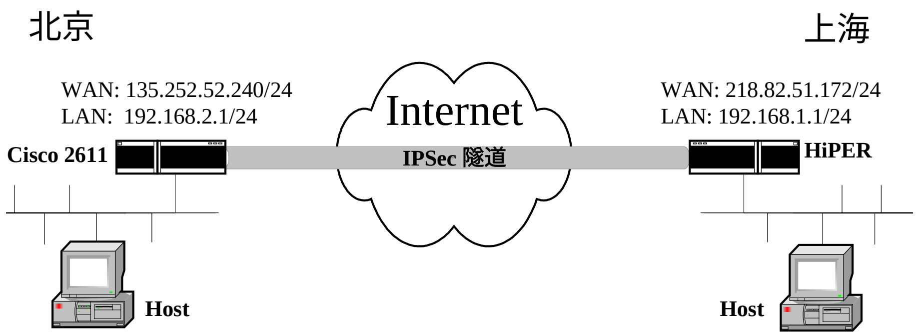


图 6-9 方案——HiPER 和 Cisco 手动方式

在本例中，如图 6-9 所示，通过使用以 DES 加密并经 MD5 认证的 ESP，采用“手动”密钥方式在上海和北京办公室之间建立 IPSec 隧道，上海使用 HiPER VPN 网关，北京使用 Cisco 2611。地址如下：

上海的 HiPER：

WAN 口： 218.82.51.172/24

静态网关：218.82.51.1/24

LAN 口： 192.168.1.1/24

北京的 Cisco 2611：

WAN 口： 135.252.52.240/24

静态网关：135.252.52.1/24

LAN 口： 192.168.2.1/24

1. 配置上海的 HiPER VPN 网关

在 ***VPN 配置—>IPSec*** 中，选择“添加”选项，然后在配置参数项中依次输入以下内容（没有列出的参数项无需配置），再单击“保存”按钮。

“设置名”： to_bj_m

“设置方式”：手动

“远端网关地址（名）”：135.252.52.240

“远端内网地址”：192.168.2.0

“远端内网掩码”：255.255.255.0

“本地绑定”：WAN（eth2）

“本地内网地址”：192.168.1.0

“本地内网掩码”：255.255.255.0

“ESP 加密算法”：DES

“ESP 加密密钥”：31323334353637383931323334353637

“ESP 认证算法”：MD5

“ESP 认证密钥”：

3132333435363738393132333435363738393132333435363738393132333435

“AH 认证算法”：NONE

“ESP 外出 SPI”：1111

“ESP 进入 SPI”：1112

2. 配置北京的 Cisco 2611 路由器

Cisco 2611 只支持 CLI 配置方式，配置如下：

//禁止使用自动 IKE，让路由器工作在手动模式

no crypto isakmp enable

//配置加密认证算法

crypto ipsec transform-set testtrans esp-des esp-md5-hmac

//配置加密认证策略，包含对端地址、SPI、加密和认证算法及密钥、需要加密的地址

crypto map manualcase 8 ipsec-manual

set peer 218.82.51.172

set session-key inbound esp 1111 cipher 31323334353637383931323334353637 authenticator 3132333435363738393132333435363738393132333435363738393132333435

set session-key outbound esp 1112 cipher 31323334353637383931323334353637 authenticator 3132333435363738393132333435363738393132333435363738393132333435

set transform-set testtrans

match address 101

//配置 Cisco 外网的接口地址

interface FastEthernet0/0

ip address 135.252.52.240 255.255.255.0

no keepalive

duplex auto

speed auto

//将加密策略应用到外网接口

crypto map manualcase

//配置 Cisco 内网的接口地址

interface FastEthernet0/1

ip address 192.168.2.1 255.255.255.0

duplex auto

speed auto

ip classless

//配置路由

ip route 0.0.0.0 0.0.0.0 135.252.52.1

//配置 ACL 表，在加密策略中引用

access-list 101 permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255

3. 查看状态

当双方配置完成，隧道建立连接并开始传输数据后，可以查看 IPSec 隧道的相关配置及状态信息。

1) 查看上海的 HiPER

对于 HiPER 来说，可以在 ***VPN 配置—>IPSec*** 中，查看“ IPSec 信息列表 ”，得到 IPSec 隧道的相关配置及状态信息，如表 6-8、表 6-9、表 6-10 所示。


IPSec 信息列表 1/16

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

	设置名	设置方式	允许	SA状态	远端网关	远端内网地址	外出加密包个数	进入解密包个数
☐	to_bj_m	手动	☑	已建立	135.252.52.240	192.168.2.1	1289	1118

表 6-8 手动（HiPER 和 Cisco）—IPSec 信息列表

IPSec 信息列表 1/16

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

本地绑定	本地内网地址	协商模式	加密认证算法	ESP外出SPI	ESP进入SPI	AH外出SPI	AH进入SPI
eth2	192.168.1.1		esp-des-md5	0x457(1111)	0x458(1112)		

表 6-9 手动（HiPER 和 Cisco）—IPSec 信息列表（续表 6-8）

IPSec 信息列表 1/16

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

法	ESP外出SPI	ESP进入SPI	AH外出SPI	AH进入SPI	生存时间(剩余)	筛选协议	筛选端口	UDP封装
d5	0x457(1111)	0x458(1112)			永久	0	0	

表 6-10 手动（HiPER 和 Cisco）—IPSec 信息列表（续表 6-9）

从表 6-8 中，可以看到“ 设置方式 ”显示为“ 手动 ”，“ SA 状态 ”显示为“ 已建立 ”，“ 外出加密包个数 ” 和 “ 进入解密包个数 ” 均有数值显示。

从表 6-9 中，可以看到“ 本地绑定 ”显示为“ eth2 ”，“ 加密认证算法 ”显示为“ esp-des-md5 ”，“ ESP 外出 SPI ” 显示为 “ 0x457（1111）”，“ ESP 进入 SPI ” 显示为 “ 0x458（1112）”。

从表 6-10 中，可以看到 “ 生存时间（剩余）” 显示为 “ 永久 ”，表示该 SA 一直有效。

2) 查看北京的 Cisco 2611

对于北京的 Cisco 2611 路由器来说，可以通过命令 *show crypto ipsec sa* 查看到隧道相关配置及状态信息，具体监控结果如下：

```
Router#show crypto ipsec sa
interface: FastEthernet0/0
    Crypto map tag: manualcase, local addr. 135.252.52.240
   local   ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   current_peer: 218.82.51.172
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 428, #pkts encrypt: 428, #pkts digest 428
    #pkts decaps: 636, #pkts decrypt: 636, #pkts verify 636
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0
     local crypto endpt.: 135.252.52.240, remote crypto endpt.: 218.82.51.172
     path mtu 1500, ip mtu 1500
     current outbound spi: 458
     inbound esp sas:
      spi: 0x457(1111)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2001, flow_id: 1, crypto map: manualcase
        no sa timing
        IV size: 8 bytes
        replay detection support: Y
```

inbound ah sas:
inbound pcp sas:
outbound esp sas:
  spi: 0x458(1112)
    transform: esp-des esp-md5-hmac ,
    in use settings ={Tunnel, }
    slot: 0, conn id: 2000, flow_id: 2, crypto map: manualcase
    no sa timing
    IV size: 8 bytes
    replay detection support: Y
outbound ah sas:
outbound pcp sas:

6.3 IPSec 自动配置实例

现实世界中应用的大量例子是自动密钥管理，正如我们前面讨论到的情况，自动密钥管理方式下，由于网关和网关的地址静态或者动态的具体情况，可以分为三种：网关到网关（也就是静态到静态），动态连接到本地（也就是对方动态，本地静态）动态连接到网关（也就是对方是静态，本地是动态）。本章节按照这三种情况分别给出配置实例。

6.3.1 网关到网关

网关到网关的形式是 IPSec 隧道的两端都具备有固定的 IP 地址。以下的例子包括了 HiPER 和 HiPER，HiPER 和 Windows XP，HiPER 和 Cisco，HiPER 和 Netscreen 等。

6.3.1.1 HiPER 和 HiPER

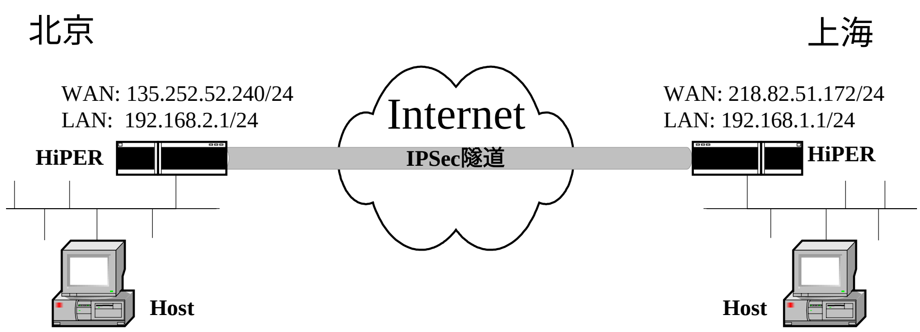


图 6-10 方案——HiPER 和 HiPER 自动方式（网关到网关）

在本例中，如图 6-10 所示，通过使用带有预共享密钥的 IKE 协议，采用“自动”密钥方式在上海和北京办公室之间建立 IPSec 隧道，上海和北京的网关都使用 HiPER VPN 网关。对“第一阶段”和“第二阶段”安全级别的配置：“第一阶段”使用 HiPER 的缺省策略，并对“第二阶段”选择策略“esp-aes256-md5-ah-sha”。预共享密钥是 testing。地址如下：

上海的 HiPER：

WAN 口： 218.82.51.172/24

静态网关：218.82.51.1/24
LAN 口： 192.168.1.1/24

北京的 HiPER：

WAN 口： 135.252.52.240/24
静态网关：135.252.52.1
LAN 口： 192.168.2.1/24

1. 配置上海的 HiPER VPN 网关

在 ***VPN 配置—>IPSec*** 中，选择“ 添加 ”选项，然后在配置参数项中依次输入以下内容（没有列出的参数项无需配置），再单击“ 保存 ”按钮。

“ 设置名 ”：sh_bj
“ 设置方式 ”：自动
“ 自动方式 ”：网关到网关
“ 远端网关地址(名) ”：135.252.52.240
“ 远端内网地址 ”：192.168.2.0
“ 远端内网掩码 ”：255.255.255.0
“ 本地绑定 ”：WAN1（eth2）
“ 本地内网地址 ”：192.168.1.0
“ 本地内网掩码 ”：255.255.255.0
“ 预共享密钥 ”（安全选项）：testing
“ 加密认证算法 1 ”（安全选项）：esp-aes256-md5-ah-sha

2. 配置北京的 HiPER VPN 网关

在 ***VPN 配置—>IPSec*** 中，选择“ 添加 ”选项，然后在配置参数项中依次输入以下内容（没有列出的参数项无需配置），再单击“ 保存 ”按钮。

“ 设置名 ”：bj_sh
“ 设置方式 ”：自动
“ 自动方式 ”：网关到网关
“ 远端网关地址（名）”：218.82.51.172
“ 远端内网地址 ”：192.168.1.0
“ 远端内网掩码 ”：255.255.255.0
“ 本地绑定 ”：WAN1（eth2）
“ 本地内网地址 ”：192.168.2.0
“ 本地内网掩码 ”：255.255.255.0
“ 预共享密钥（安全选项）”：testing
“ 加密认证算法 1（安全选项）”：esp-aes256-md5-ah-sha

3. 查看状态

当双方配置完成后，上海和北京的 HiPER 通过流量或者手工触发建立起 IPSec 隧道。可以在 ***VPN 配置—>IPSec*** 中，查看“ IPSec 信息列表 ”，得到 IPSec 隧道的相关配置及状态信息，如表 6-11、表 6-12、表 6-13 所示（此处以上海的 HiPER 为例进行说明，北京的 HiPER 类似）。

IPSec 信息列表 1/500

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

	设置名	设置方式	允许	SA状态	远端网关	远端内网地址	外出加密包个数	进入解密包个数	本地绑定	本
☐	sh_bj	自动	☑	已建立	135.252.52.240	192.168.2.1	10480	10480	eth2	

表 6-11 网关到网关（HiPER 和 HiPER）—IPSec 信息列表

IPSec 信息列表 1/500

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

本地内网地址	协商模式	加密认证算法	ESP外出SPI	ESP进入SPI	A
192.168.1.1	主模式	esp-aes256-md5-ah-sha	0x22c4e319(583328537)	0x2d8521e8(763699688)	0x22c4e

表 6-12 网关到网关（HiPER 和 HiPER）—IPSec 信息列表（续表 6-11）

IPSec 信息列表 1/500

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

进入SPI	AH外出SPI	AH进入SPI	生存时间(剩余)	筛选协议	筛选端口	UDP封装
3(763699688)	0x22c4e318(583328536)	0x2d8521e7(763699687)	00:00:59:02	0	0	

表 6-13 网关到网关（HiPER 和 HiPER）—IPSec 信息列表（续表 6-12）

从表 6-11 中，可以看到“设置方式”显示为“自动”，“SA 状态”显示为“已建立”，“外出加密包个数”和“进入解密包个数”均有数值显示，“本地绑定”显示为“eth2”。

从表 6-12 中，可以看到“协商模式”显示为“主模式”，“加密认证算法”显示为“esp-aes256-md5-ah-sha”，“ESP 外出 SPI”、“ESP 进入 SPI”、“AH 外出 SPI”及“AH 进入 SPI”均显示为自动协商时得到的数值。

从表 6-13 中，可以看到“生存时间（剩余）”显示为“00:00:59:02”，表示该 SA 的剩余有效时间为 59 分 02 秒。

6.3.1.2 HiPER 和 Windows 2000



图 6-11 方案——HiPER 和 Windows 2000 自动方式（网关到网关）

在本例中，如图 6-11 所示，通过使用带有预共享密钥的 IKE 协议，采用“自动”密钥方式在 HiPER VPN 网关和 Windows 2000 之间建立 IPSec 隧道。预共享密钥是 hiper123。地址如下：

HiPER：

WAN 口：200.200.200.134/24

LAN 口： 192.168.1.133/24

Windows 2000：

第一块网卡：200.200.200.200/24
第二块网卡：192.168.111.3/24

1. 配置 HiPER VPN 网关

在 ***VPN 配置—>IPSec*** 中，选择“添加”选项，然后在配置参数项中依次输入以下内容（没有列出的参数项无需配置），再单击“保存”按钮。

“设置名”：to_win2K
“设置方式”：自动
“自动方式”：网关到网关
“远端网关地址（名）”：200.200.200.200
“远端内网地址”：192.168.111.0
“远端内网掩码”：255.255.255.0
“本地绑定”：WAN1（eth2）
“本地内网地址”：192.168.1.0
“本地内网掩码”：255.255.255.0
“预共享密钥（安全选项）”：hiper123
“加密认证算法 1（安全选项）”：esp-3des-sha

2. 配置 Windows 2000

1) 点击 Windows 2000 的“开始”→“运行”，输入命令：secpol.msc。
2) 右击“IP 安全策略，在本地计算机”，选择“创建 IP 安全策略”。
3) 单击“下一步”按钮，在“名称”中输入“to_hiper IPSec Policy”，也可以在“描述”中输入更多的内容。
4) 取消“激活默认响应规则”的选中，单击“下一步”按钮。
5) 保留选项“编辑属性”的选中，单击“完成”按钮。
6) 配置密钥交换内容：
   a) 右击“to_hiper IPSec Policy”，然后选择“属性”。
   b) 在“常规”属性页面，单击“高级”选项，进入“密钥交换设置”界面，如图 6-12 所示。

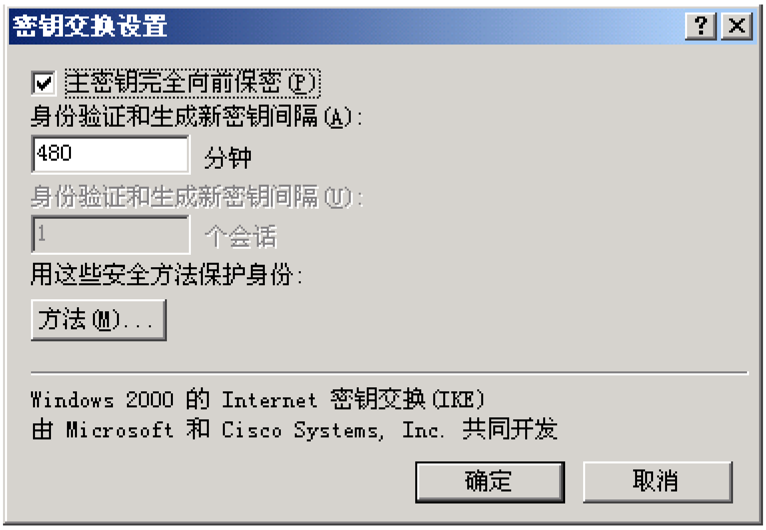


图 6-12 密钥交换设置界面

   c) 查看密钥的生存时间，选中“主密钥完全向前保密”。
   d) 单击“方法”按钮，进入页面“密钥交换安全措施”，保留第一条措施，其余

删除。

e) 单击“编辑”按钮，进入“IKE 安全算法”界面（如图 6-13），编辑 IKE 的策略：“完整性算法”选择 SHA1，“加密算法”选择“3DES”，“Diffie-Hellman 小组”选择“中（2）”。



图 6-13 IKE 安全算法界面

f) 保存上述配置，并关闭“to_hiper IPSec Policy 属性”界面。

7) 创建 win2K 到 HiPER 的 IP Filter 列表：

a) 右击“IP 安全策略，在本地计算机”，单击“管理 IP 筛选器表和筛选器操作”。

b) 进入“管理 IP 筛选器列表”页面，单击“添加”按钮。

c) 在“名称”中输入“win2K to hiper IP Filter List”，也可在“描述”输入更多的内容。

d) 选择“使用“添加向导””选项，并单击“添加”按钮。

e) 在“IP 筛选器向导”界面，单击“下一步”按钮，进入如图 6-14 所示界面。

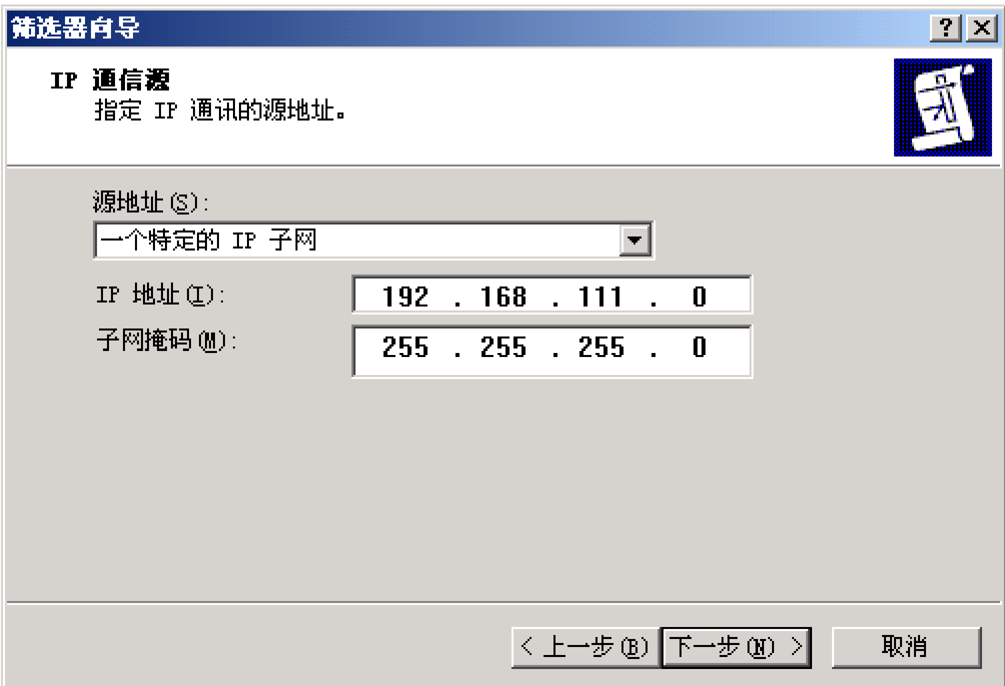


图 6-14 筛选器向导（IP 通信源）界面

f) 在“源地址”中选择“一个特定的 IP 子网”，在“IP 地址”中输入“192.168.111.0”，在“子网掩码”中输入“255.255.255.0”，单击“下一步”按钮，进入如图 6-15

所示界面。



图 6-15 筛选器向导（IP 通信目标）界面

g） 在“目标地址”中选择“一个特定的 IP 子网”，在“IP 地址”中输入“192.168.1.0”，在“子网掩码”中输入“255.255.255.0”，单击“下一步”按钮，进入如图 6-16 所示界面。

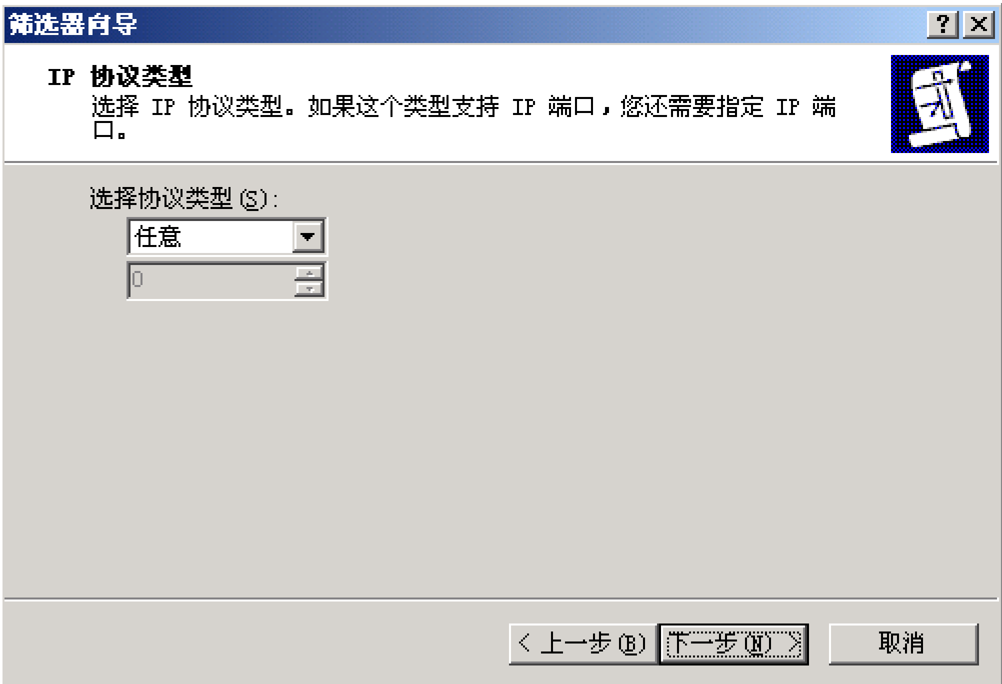


图 6-16 筛选器向导（IP 协议类型）界面

h） 在“选择协议类型”中选择“任意”，单击“下一步”按钮。

i） 选中“编辑属性”，单击“完成”按钮。

j） 在“筛选器属性”界面，如图 6-17 所示，禁用“镜像”，单击“确定”按钮。

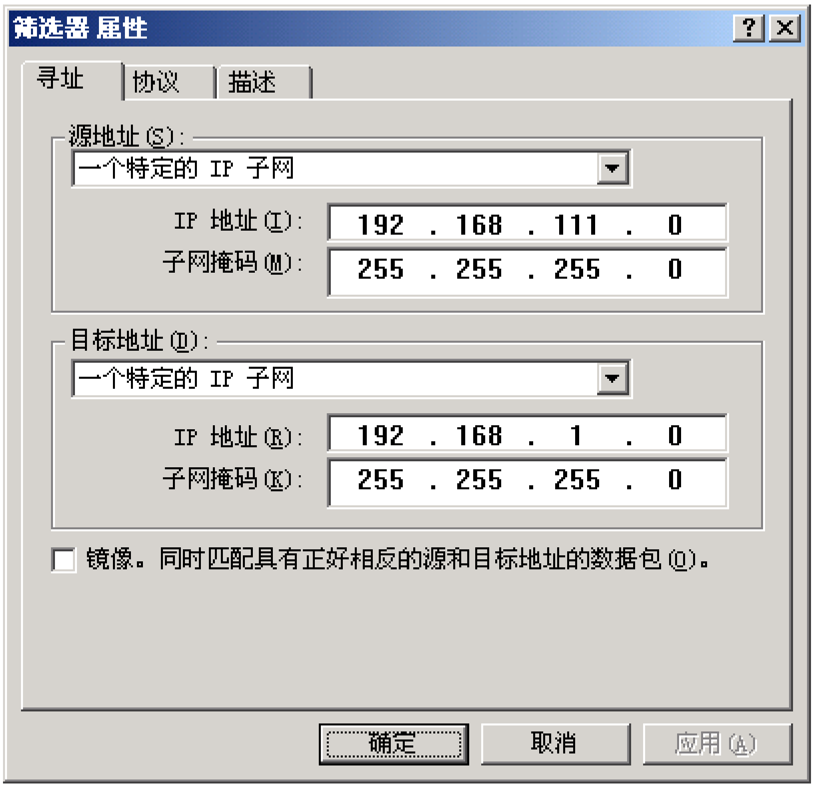


图 6-17 筛选器属性（寻址）界面（一）

8) 创建 HiPER 到 win2K 的 IP Filter 列表

a) 右击“ IP 安全策略，在本地计算机 ”，单击“ 管理 IP 筛选器表和筛选器操作 ”。

b) 进入“ 管理 IP 筛选器列表 ” 页面，单击“ 添加 ” 按钮。

c) 在“ 名称 ” 中输入“ hiper to win2K IP Filter ”，也可在“ 描述 ” 输入更多的内容。

d) 选择“ 使用“ 添加向导 ”” 选项，并单击“ 添加 ” 按钮。

e) 在“ IP 筛选向导 ” 页面，单击“ 下一步 ” 按钮。

f) 在“ 源地址 ”中选择“ 一个特定的 IP 子网 ”，在“ IP 地址 ”中输入“ 192.168.1.0 ”，在“ 子网掩码 ” 中输入“ 255.255.255.0 ”，单击“ 下一步 ” 按钮。

g) 在“ 目标地址 ”中选择“ 一个特定的 IP 子网 ”，在“ IP 地址 ”中输入“ 192.168.111.0 ”，在“ 子网掩码 ” 中输入“ 255.255.255.0 ”，单击“ 下一步 ” 按钮。

h) 在“ 选择协议类型 ” 中选择“ 任意 ”，单击“ 下一步 ” 按钮。

i) 选中“ 编辑属性 ”，单击“ 完成 ” 按钮。

j) 在“ 筛选器属性 ” 界面，如图 6-18 所示，禁用“ 镜像 ”，单击“ 确定 ” 按钮。

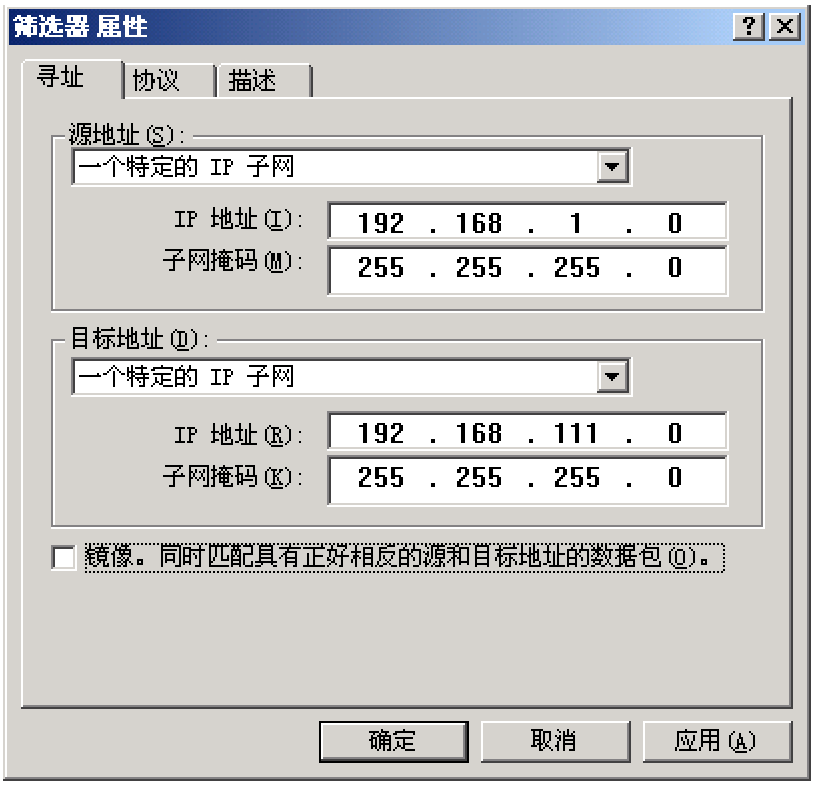


图 6-18 筛选器属性（寻址）界面（二）

9) 创建 win2K 到 HiPER 的 Filter 动作

a) 右击“ IP 安全策略，在本地计算机 ”，选择“ 管理 IP 筛选器表和筛选器操作 ”。

b) 进入“ 管理筛选器操作 ” 页面。

c) 取消“ 使用“ 添加向导 ”” 选项的选中，并单击“ 添加 ” 按钮。

d) 进入“ 安全措施 ” 属性页面，选择“ 协商安全 ”，并单击“ 添加 ” 按钮。

e) 选择“ 自定义 ”，并单击“ 设置 ” 按钮，进入如图 6-19 所示界面。

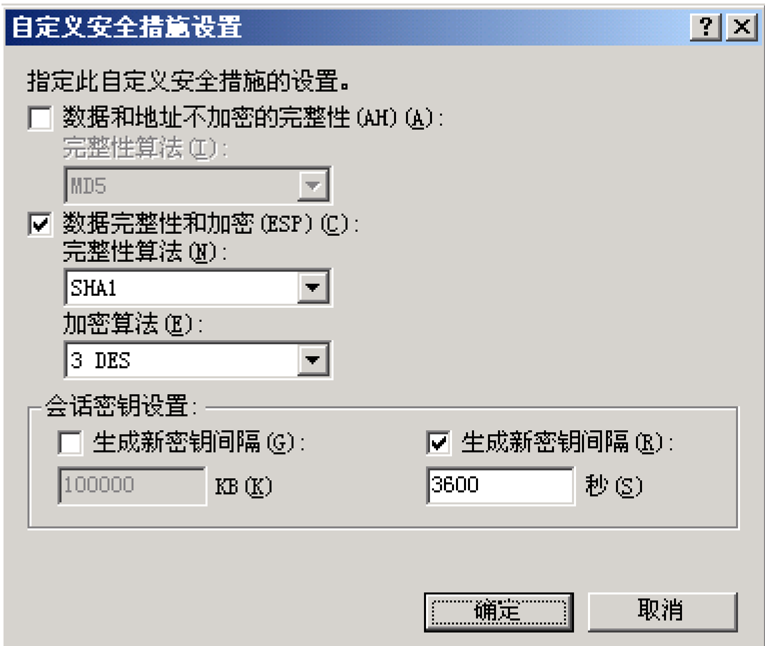


图 6-19 自定义安全措施设置界面

f) 选中“数据完整性和加密（ESP）”，同时“完整性算法”选择“SHA1”，“加密算法”选择“3DES”。

g) 选中“生成新密钥间隔”，并保持为缺省值 3600 秒。

h) 保存配置生效，回到“管理筛选器操作”界面。

i) 选中“新筛选器操作”，单击“编辑”按钮，进入如图 6-20 所示界面。

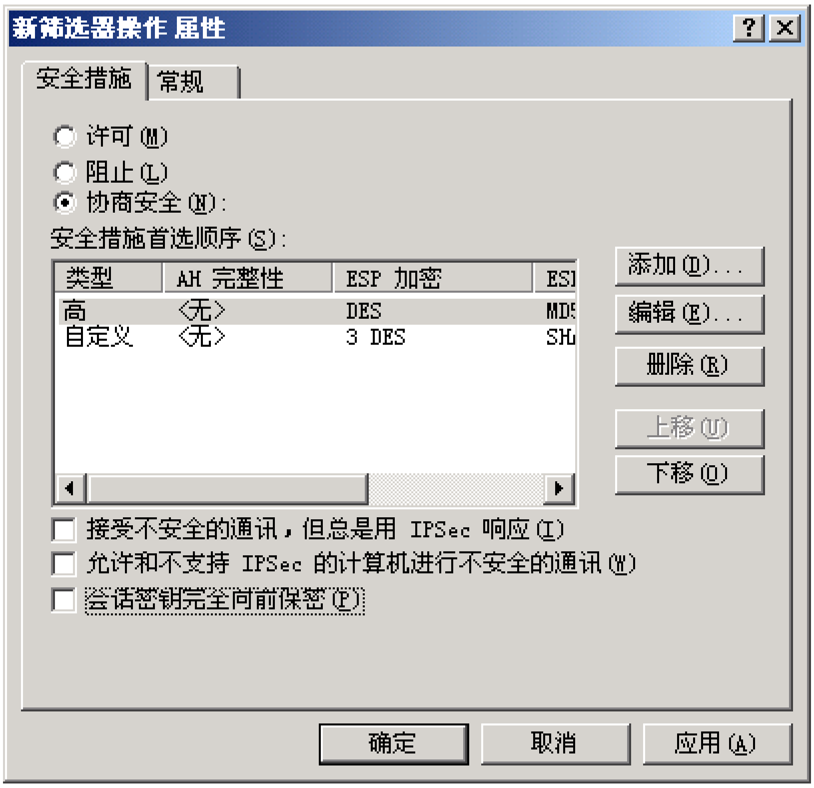


图 6-20 新筛选操作属性（安全措施）界面

j) 确保选项“接受不安全的通讯，但总是用 IPSec 响应”和“允许和不支持 IPSec 的计算机进行不安全的通讯”及“会话密钥完全向前保密”未被选中。

k) 进入“常规”属性界面（图 6-21），在“名称”中填入“win2K to hiper Filter Action”，单击“确定”按钮。

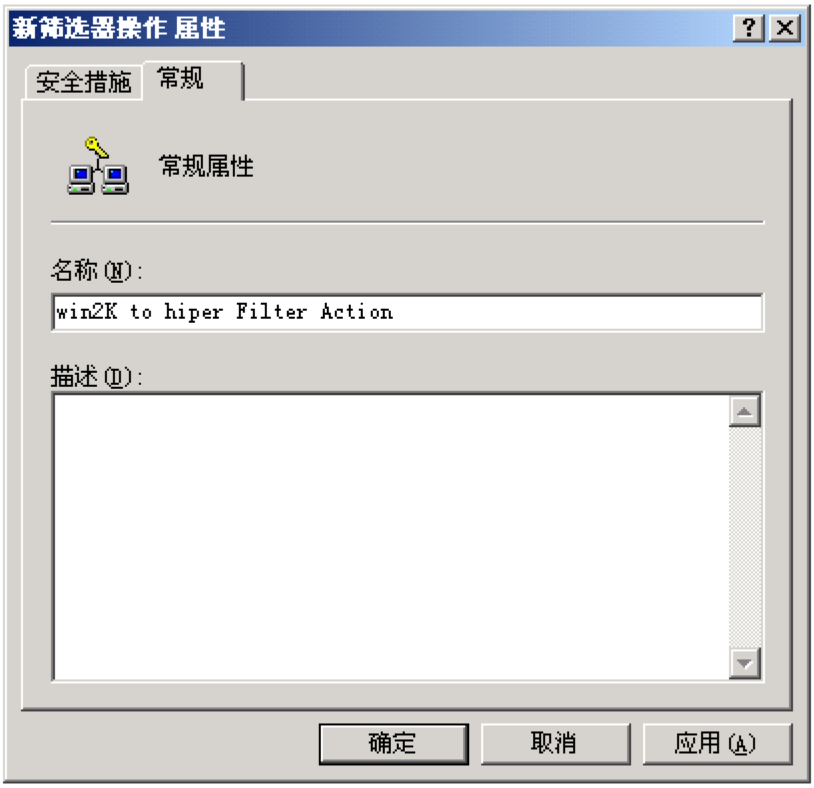


图 6-21 新筛选操作属性（常规）界面

10) 创建 win2000 到 HiPER 的隧道规则

a) 双击“ to_hiper IPSec Policy ”，进入“ 规则 ”属性页面。

b) 选中“ 使用“ 添加向导 ”” 选项，单击“ 添加 ” 按钮，单击“ 下一步 ” 按钮，进入如图 6-22 所示界面，选中“ 隧道终点由此 IP 地址指定 ”，填入“ 200.200.200.134 ”。

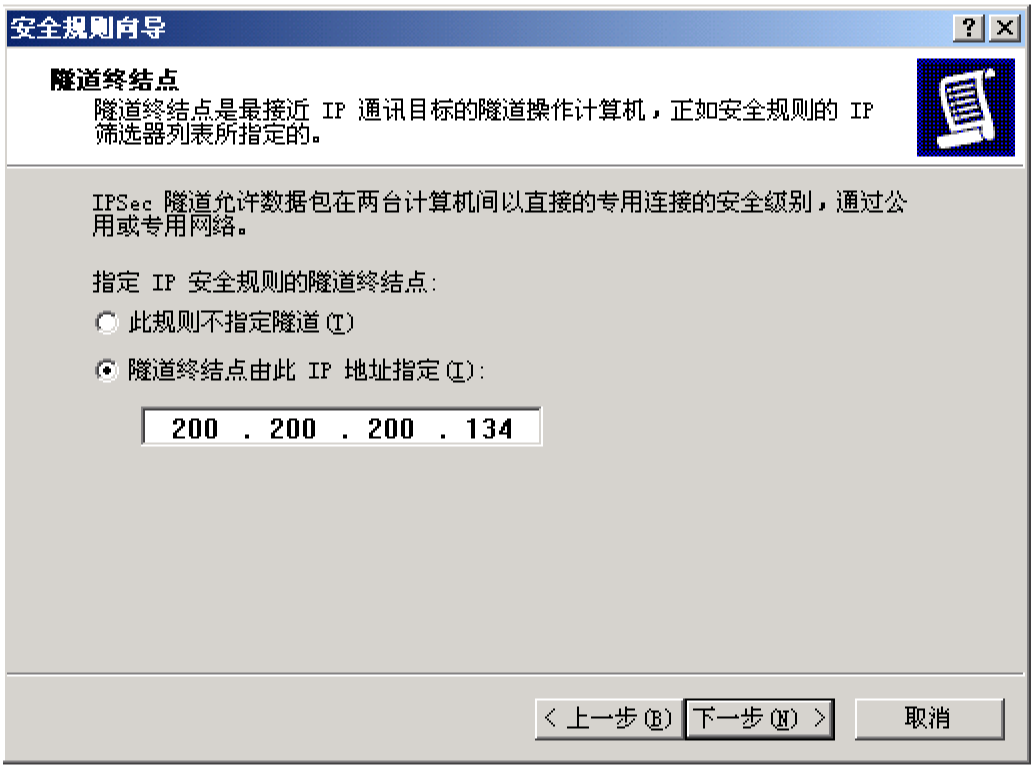


图 6-22 安全规则向导界面（一）

c） 单击“ 下一步 ”按钮，进入如图 6-22 所示界面，选中“ 局域网（LAN）”。

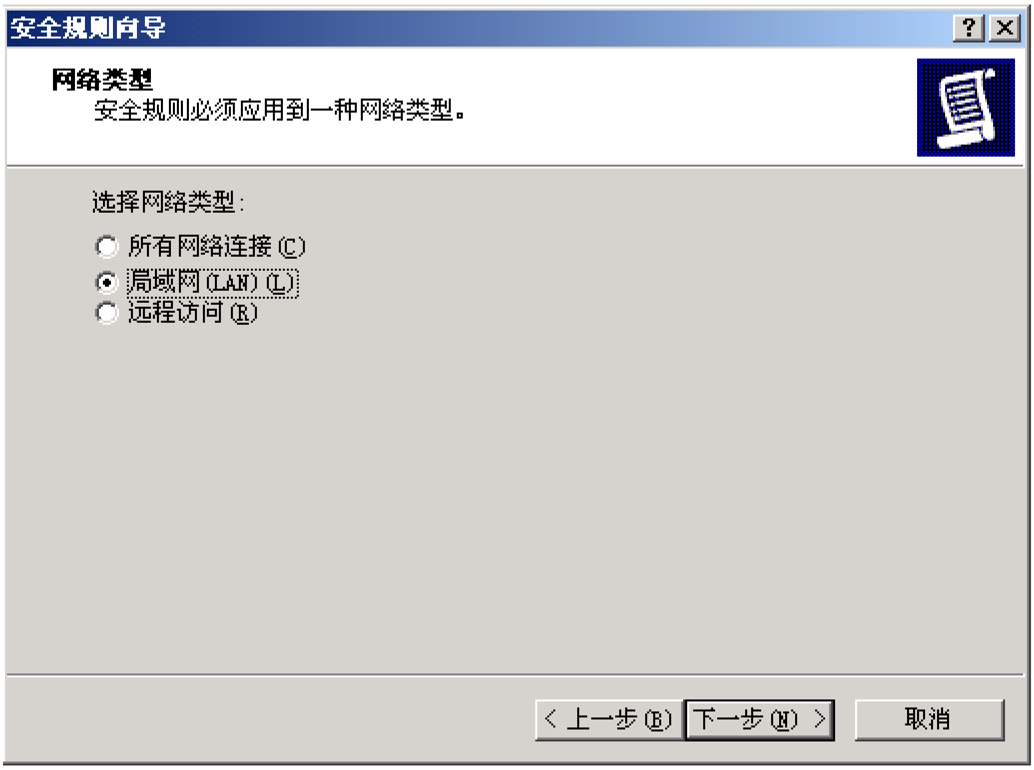


图 6-23 安全规则向导界面（二）

d） 单击“ 下一步 ”按钮，进入如图 6-24 所示界面，选中“ 此字符串用来保护密钥交换（预共享密钥）”，并填入“ hiper123 ”作为预共享密钥值。

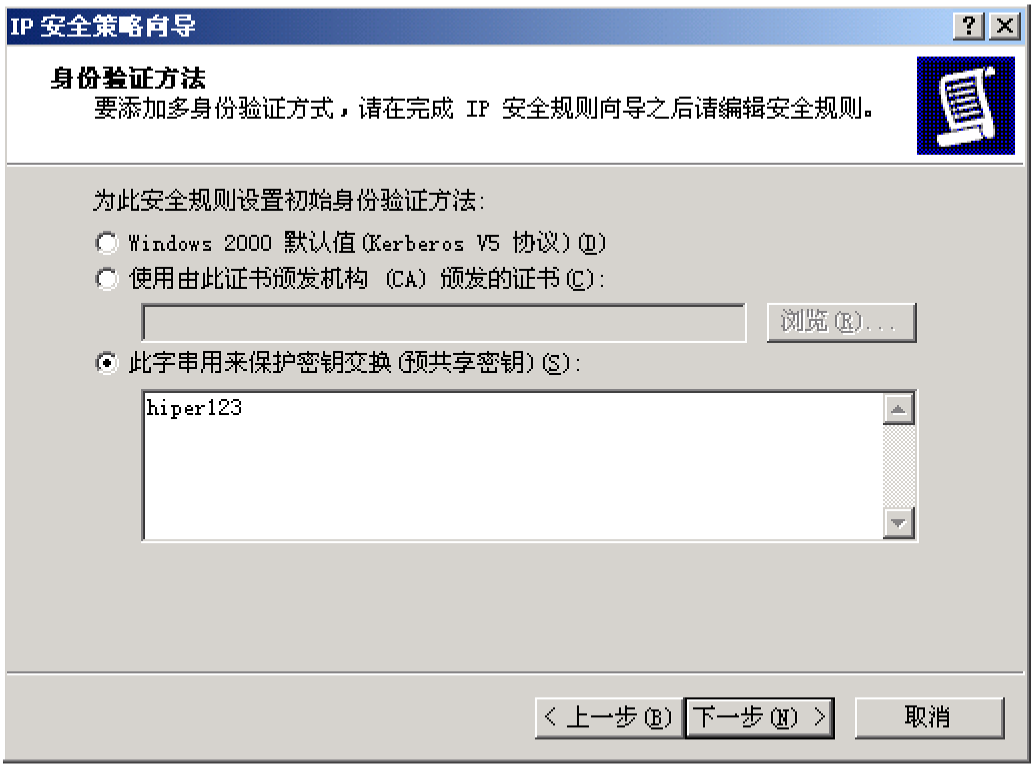


图 6-24 IP 安全策略向导界面

e) 单击“下一步”按钮，进入如图 6-25 所示界面，在“IP 筛选器列表”中选中“win2K to hiper IP Filter”。

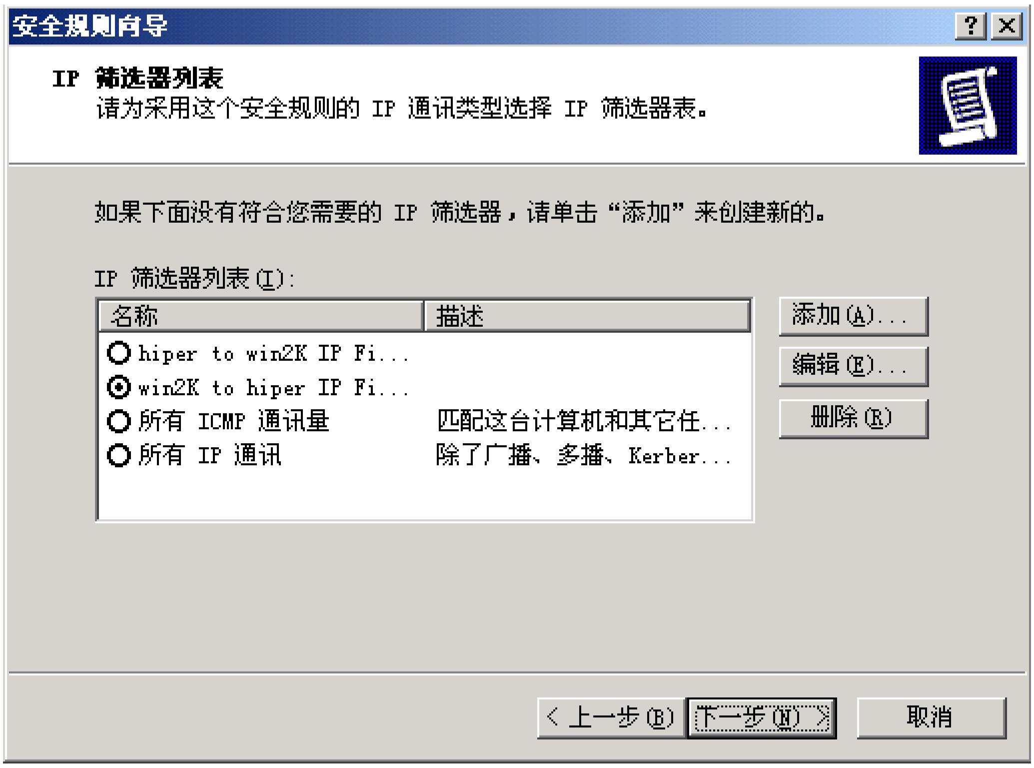


图 6-25 安全规则向导界面（三）

f) 单击“下一步”按钮，进入如图 6-26 所示界面，在“IP 筛选器列表”中选中“win2K to hiper Filter Action”。

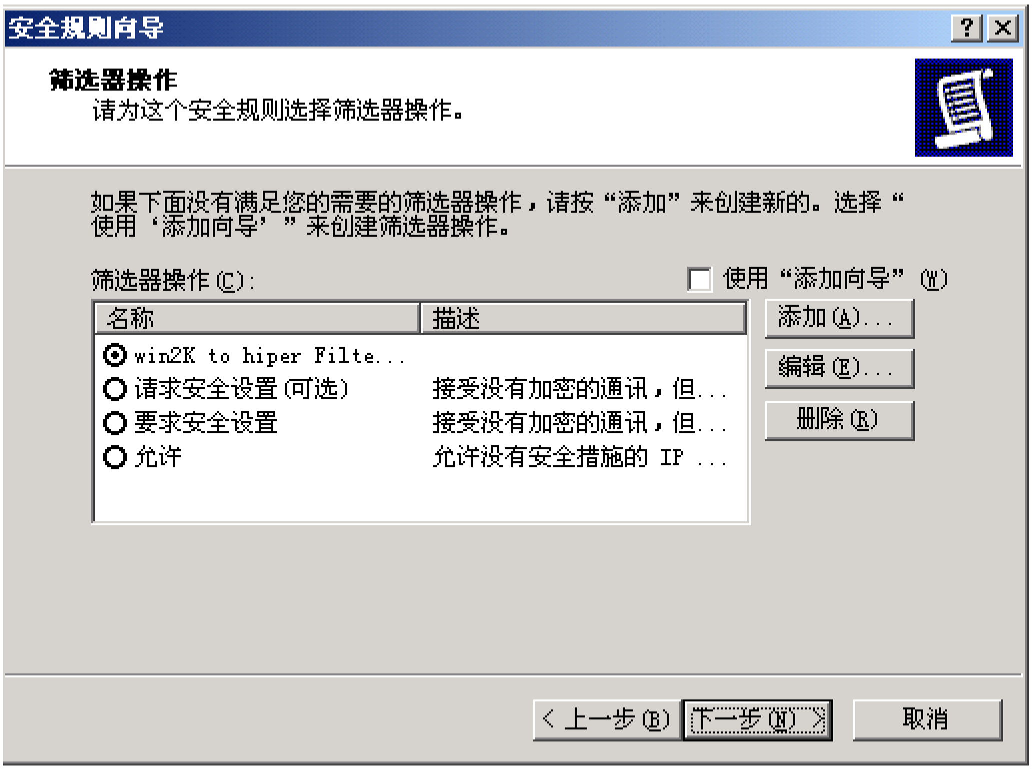


图 6-26 安全规则向导界面（四）

g） 保存所设配置，使配置生效。

11) 创建 HiPER 到 win2000 隧道规则

a） 双击“ to_hiper IPSec Policy ”，进入“ 规则 ”属性页面。

b） 选中“ 使用“ 添加向导 ”” 选项，单击“ 添加 ”按钮，单击“ 下一步 ”按钮，选中“ 隧道终点由此 IP 地址指定 ”，填入“ 200.200.200.200 ”。

c） 单击“ 下一步 ”按钮，“ 网络类型 ”选则“ 局域网（LAN）。

d） 单击“ 下一步 ”按钮，选中“ 此字符串用来保护密钥交换（预共享密钥）”，并填入“ hiper123 ”作为预共享密钥值。

e） 单击“ 下一步 ”按钮，在“ IP 筛选器列表 ”中选中“ hiper to win2K IP Filter ”。

f） 单击“ 下一步 ”按钮，在“ IP 筛选器列表 ”中选中“ win2K to hiper Filter Action ”。

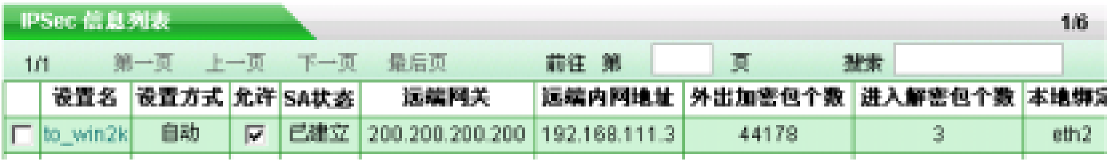
g） 保存所设配置，使配置生效。

12) 激活 win2000 到 HiPER 的 IPSec 策略

右击“ to_hiper IPSec Policy ”，单击“ 指派 ”，策略激活。

3. 查看状态

当双方配置完成后，HiPER 和 Windows 2000 通过流量或者手工触发建立起 IPSec 隧道。对于 HiPER 来说，可以在 ***VPN 配置—>IPSec*** 中，查看“ IPSec 信息列表 ”，得到 IPSec 隧道的相关配置及状态信息，如表 6-14、表 6-15、表 6-16 所示所示。



IPSec 信息列表 1/6

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

	设置名	设置方式	允许	SA状态	远端网关	远端内网地址	外出加密包个数	进入解密包个数	本地绑
☐	to_win2k	自动	☑	已建立	200.200.200.200	192.168.111.3	44178	3	eth2

表 6-14 网关到网关（HiPER 和 Win2000）—IPSec 信息列表

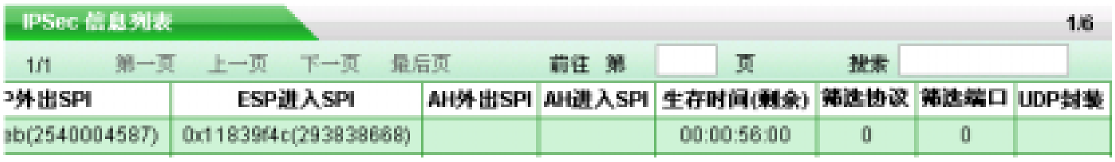


IPSec 信息列表 1/6

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

本地绑定	本地内网地址	协商模式	加密认证算法	ESP外出SPI	ESP进入SPI	AH外出
eth2	192.168.1.133	主模式	esp-3des-sha	0x976564eb(2540004587)	0x11839f4c(293838668)	

表 6-15 网关到网关（HiPER 和 Win2000）—IPSec 信息列表（续表 6-14）



IPSec 信息列表 1/6

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

外出SPI	ESP进入SPI	AH外出SPI	AH进入SPI	生存时间(剩余)	筛选协议	筛选端口	UDP封装
ab(2540004587)	0x11839f4c(293838668)			00:00:56:00	0	0	

表 6-16 网关到网关（HiPER 和 Win2000）—IPSec 信息列表（续表 6-15）

从表 6-14 中，可以看到“ 设置方式 ”显示为“ 自动 ”，“ SA 状态 ”显示为“ 已建立 ”，“ 外出加密包个数 ”和“ 进入解密包个数 ”均有数值显示。

从表 6-15 中，可以看到“ 本地绑定 ”显示为“ eth2 ”，“ 协商模式 ”显示为“ 主模式 ”，“ 加密认证算法 ”显示为“ esp-3des-sha ”，“ ESP 外出 SPI ”和“ ESP 进入 SPI ”显示为自动协商时得到的数值。

从表 6-16 中，可以看到“ 生存时间（剩余）”显示为“ 00:00:56:00 ”，表示该 SA 的剩余有效时间为 56 分 00 秒。

6.3.1.3 HiPER 和 Cisco

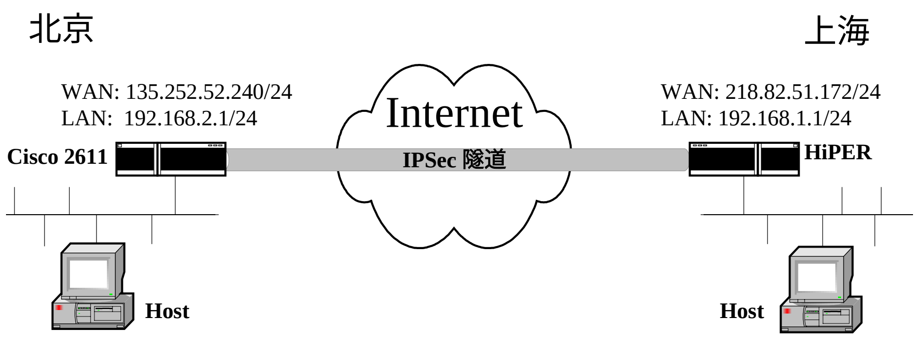


图 6-27 方案——HiPER 和 Cisco 自动方式（网关到网关）

在本例中，如图 6-27 所示，通过使用带有预共享密钥的 IKE 协议，采用“自动”密钥方式在上海和北京办公室之间建立 IPSec 隧道，在上海使用 HiPER VPN 网关，在北京使用 Cisco 2611 路由器，预共享密钥是 testing。地址如下：

上海的 HiPER：

WAN 口： 218.82.51.172/24

静态网关：218.82.51.1/24

LAN 口： 192.168.1.1/24

北京的 cisco 2611：

WAN 口： 135.252.52.240/24

静态网关：135.252.52.1

LAN 口： 192.168.2.1/24

1. 配置上海的 HiPER VPN 网关

在 ***VPN 配置—>IPSec*** 中，选择“添加”选项，然后在配置参数项中依次输入以下内容（没有列出的参数项无需配置），再单击“保存”按钮。

“设置名”：to_Cisco

“设置方式”：自动

“自动方式”：网关到网关

“远端网关地址（名）”：135.252.52.240

“远端内网地址”：192.168.2.0

“远端内网掩码”：255.255.255.0

“本地绑定”：WAN（eth2）

“本地内网地址”：192.168.1.0

“本地内网掩码”：255.255.255.0

“预共享密钥”（安全选项）：testing

“加密认证算法 1”（安全选项）：esp-des-sha

2. 配置北京的 Cisco 2611 路由器

Cisco 2611 只支持 CLI 配置方式，配置如下：

//配置第一阶段安全策略

crypto isakmp policy 1

hash md5

authentication pre-share

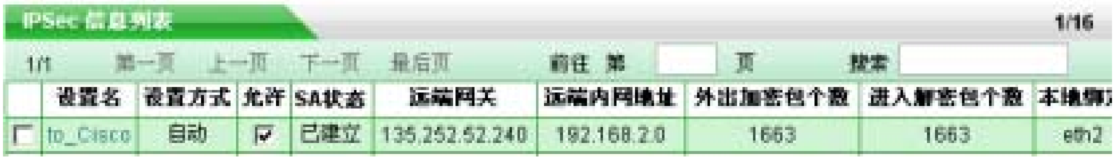
```
  group 2
//配置和对方的预共享密钥
 crypto isakmp key testing address 218.82.51.172
//配置第二阶段加密认证算法
 crypto ipsec transform-set hiper esp-des esp-sha-hmac
//配置第二阶段安全策略
 crypto map hipermap 10 ipsec-isakmp
  set peer 218.82.51.172
  set transform-set hiper
  match address 101
//配置外网的接口地址
 interface FastEthernet0/0
  ip address 135.252.52.240 255.255.255.0
  no keepalive
  duplex auto
  speed auto
//将安全策略应用到外网接口
 crypto map hipermap
//配置内网的接口地址
 interface FastEthernet0/1
  ip address 192.168.2.1 255.255.255.0
  duplex auto
  speed auto
 ip classless
//配置路由
 ip route 0.0.0.0 0.0.0.0 135.252.52.1
//配置 ACL 表，在安全策略中引用
 access-list 101 permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
```

3. 查看状态

当双方配置完成，上海的 HiPER 和北京的 Cisco 通过流量或者手工触发建立起 IPSec 隧道后，可以查看 IPSec 隧道的相关配置及状态信息。

1) 查看上海的 HiPER

对于上海的 HiPER 来说，可以在 ***VPN 配置—>IPSec*** 中，查看 " IPSec 信息列表 "，得到 IPSec 隧道的相关配置及状态信息，如表 6-17、表 6-18、表 6-19 所示。


IPSec 信息列表 1/16
1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

	设置名	设置方式	允许	SA状态	远端网关	远端内网地址	外出加密包个数	进入解密包个数	本地绑
☐	to_Cisco	自动	☑	已建立	135.252.52.240	192.168.2.0	1663	1663	eth2

表 6-17 网关到网关（HiPER 和 Cisco）—IPSec 信息列表

IPSec 信息列表 1/16

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

本地内网地址	协商模式	加密认证算法	ESP外出SPI	ESP进入SPI	AH外出SPI	AH进入
192.168.1.0	主模式	esp-des-sha	0x3b61f3bd(996275133)	0x40f05ef3(1089494771)		

表 6-18 网关到网关（HiPER 和 Cisco）—IPSec 信息列表（续表 6-17）

IPSec 信息列表 1/16

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

外出SPI	ESP进入SPI	AH外出SPI	AH进入SPI	生存时间(剩余)	筛选协议	筛选端口	UDP封装
bd(996275133)	0x40f05ef3(1089494771)			00:00:51:01	0	0	

表 6-19 网关到网关（HiPER 和 Cisco）—IPSec 信息列表（续表 6-18）

从表 6-17 中，可以看到“设置方式”显示为“自动”，“SA 状态”显示为“已建立”，“外出加密包个数”和“进入解密包个数”均有数值显示。

从表 6-18 中，可以看到“本地绑定”显示为“eth2”，“协商模式”显示为“主模式”，“加密认证算法”显示为“esp-des-sha”，“ESP 外出 SPI”和“ESP 进入 SPI”显示为自动协商时得到的数值。

从表 6-19 中，可以看到“生存时间（剩余）”显示为“00:00:51:01”，表示该 SA 的剩余有效时间为 51 分 01 秒。

2) 查看北京的 Cisco 2611

对于北京的 Cisco 2611 路由器来说，可以通过命令 *show crypto ipsec sa* 查看到隧道相关配置及状态信息，具体监控结果如下：

```
hiperr# show crypto ipsec sa
interface: FastEthernet0/0
    Crypto map tag: hipermap, local addr. 135.252.52.240
  local   ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
  current_peer: 218.82.51.172
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 1667, #pkts encrypt: 1667, #pkts digest 1667
    #pkts decaps: 1626, #pkts decrypt: 1626, #pkts verify 1626
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
    #send errors 1, #recv errors 0
     local crypto endpt.: 135.252.52.240, remote crypto endpt.: 218.82.51.172
     path mtu 1500, ip mtu 1500
     current outbound spi: 2971F16D
     inbound esp sas:
      spi: 0x3bb1f3bd(146951604)
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: hipermap
        sa timing: remaining key lifetime (k/sec): (4607515/3072)
        IV size: 8 bytes
```

replay detection support: Y
inbound ah sas:
inbound pcp sas:
outbound esp sas:
spi: 0x40f053f3(695333229)
transform: esp-des esp-sha-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2001, flow_id: 2, crypto map: hipermap
sa timing: remaining key lifetime (k/sec): (4607359/3072)
IV size: 8 bytes
replay detection support: Y
outbound ah sas:
outbound pcp sas:

6.3.1.4 HiPER 和 Netscreen



图 6-28 方案——HiPER and Netscreen 自动方式（网关到网关）

在本例中，如图 6-28 所示，通过使用带有预共享密钥的 IKE 协议，采用“自动”密钥方式在上海和北京办公室之间建立 IPSec 隧道，在上海使用 HiPER VPN 网关，通过 ADSL 接入，使用 PPPoE 拨号得到静态地址；在北京使用 Netscreen。预共享密钥是 h1i2p3e4r5。地址如下：

上海的 HiPER：
WAN 口： 218.80.107.110/24
静态网关：218.80.107.110/24
LAN 口： 192.168.20.1/24

北京的 Netscreen：
ethernet3 口：202.101.36.46/24
静态网关： 202.101.36.1/24
LAN 口： 192.168.2.1/24

1. 配置上海的 HiPER VPN 网关

在 ***VPN 配置—>IPSec*** 中，选择“添加”选项，然后在配置参数项中依次输入以下内容（没有列出的参数项无需配置），再单击“保存”按钮。

“设置名”：sh_to_bj
“设置方式”：自动
“自动方式”：网关到网关

"远端网关地址(名)"：202.101.36.46
"远端内网地址"：192.168.2.0
"远端内网掩码"：255.255.255.0
"本地绑定"：PPPOE
"本地内网地址"：192.168.20.0
"本地内网掩码"：255.255.255.0
"预共享密钥"（安全选项）：h1i2p3e4r5
"加密认证算法 1"（安全选项）：esp-3des-sha

2. 配置北京的 Netscreen
这里只给出基于 WEB UI 方式下配置 Netscreen 的方法。

配置接口－ 安全区段

1) 进入"Network"→"Interfaces"，单击"ethernet7 "后的"Edit"超链接，输入以下内容，然后单击"OK"按钮。
"Zone Name"：Trust
"IP Address/Netmask"：192.168.2.1/24
2) 进入"Network"→"Interfaces"，单击"ethernet3"后的"Edit"超链接，输入以下内容，然后单击"OK"按钮。
"Zone Name"：Untrust
"IP Address/Netmask"：202.101.36.46/24

配置地址

3) 进入"Objects"→"Addresses"→" List"，单击"New"按钮，再输入以下内容，然后单击"OK"按钮。
"Address Name"：Trust_LAN
"IP Address/Domain Name"：选中"IP/Netmask"
"IP/Netmask"：192.168.2.0/24
"Zone"：Trust
4) 进入"Objects"→"Addresses"→" List"，单击"New"按钮，再输入以下内容，然后单击"OK"按钮。
"Address Name"：sh_office
"IP Address/Domain Name"：选中"IP/Netmask"
"IP/Netmask"：192.168.20.0/24
"Zone"：Untrust

配置 VPN

5) 进入"VPNs"→"AutoKey Advanced"→"Gateway"，单击"New"按钮，再输入以下内容。
"Gateway Name"：To_shanghai
"Security Level"：Custom
"Remote Gateway Type"：选中"Static IP Address"
"IP Address/Hostname"：218.80.107.110
"Preshared Key"：h1i2p3e4r5
"Outgoing Interface"：ethernet3
单击"Advanced"按钮，再输入以下高级设置参数：
"Security Level"：Custom

"Phase 1 Proposal"：pre-g2-3des-sha
"Mode（Initiator）"：Main
然后单击"Return"按钮，返回到上一页，再单击"OK"按钮。

6) 进入"VPNs"→"AutoKey IKE"，单击"New"按钮，再输入以下内容，然后单击"OK"按钮。
"VPN Name"：corp_branch
"Security Level"：Compatible
"Remote Gateway"：选中"Predefined"
"Predefined"：To_shanghai

配置路由

7) 进入"Network"→"Routing"→"Routing Table"，选中"trust-vr"，单击"New"按钮，再输入以下内容，然后单击"OK"按钮。
"Network Address/Netmask"：0.0.0.0/0
"Gateway"：选中
"Interface"：ethernet3（untrust）
"Gateway IP Address"：202.101.36.1

配置策略

8) 进入"Policies"，"From"选中"Trust"，"To"选中"Untrust"，单击"New"按钮，再输入以下内容，然后单击"OK"按钮。
"Source Address"：选中"Address Book"
"Address Book"：Trust_lan
"Destination Address"：选中"Address Book"
"Address Book"：sh_office
"Service"：ANY
"Action"：Tunnel
"VPN Tunnel"：corp_branch
"Modify matching VPN policy"：选中
"Position at Top"：选中

3. 查看状态

当双方配置完成后，上海的 HiPER 和北京的 Netscreen 通过流量或者手工触发建立起 IPSec 隧道。

1) 查看上海的 HiPER

对于上海的 HiPER 来说，可以在 ***VPN 配置—>IPSec*** 中，查看"IPSec 信息列表"，得到 IPSec 隧道的相关配置及状态信息，如表 6-20、表 6-21、表 6-22 所示。

IPSec 信息列表 1/16

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

	设置名	设置方式	允许	SA状态	远端网关	远端内网地址	外出加密包个数	进入解密包个数	本地绑定
☐	sh_to_bj	自动	☑	已建立	202.101.36.46	192.168.2.0	1721	1721	PPPOE

表 6-20 网关到网关（HiPER 和 Netscreen）—IPSec 信息列表

IPSec 信息列表 1/16

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

本地内网地址	协商模式	加密认证算法	ESP外出SPI	ESP进入SPI	AH外出SPI	AH进
192.168.20.1	主模式	esp-3des-sha	0x115820fe(290988286)	0xb9b84f1b(3115863835)		

表 6-21 网关到网关（HiPER 和 Netscreen）—IPSec 信息列表（续表 6-20）

IPSec 信息列表 1/16

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

外出SPI	ESP进入SPI	AH外出SPI	AH进入SPI	生存时间(剩余)	筛选协议	筛选端口	UDP封装
(290988286)	0xb9b84f1b(3115863835)			00:00:53:12	0	0	

表 6-22 网关到网关（HiPER 和 Netscreen）—IPSec 信息列表（续表 6-21）

从表 6-20 中，可以看到“设置方式”显示为“自动”，“SA 状态”显示为“已建立”，“外出加密包个数”和“进入解密包个数”均有数值显示，可以看到“本地绑定”显示为“PPPOE”。

从表 6-21 中，可以看到 “协商模式”显示为“主模式”，“加密认证算法”显示为“esp-3des-sha”，“ESP 外出 SPI”和“ESP 进入 SPI”显示为自动协商时得到的数值。

从表 6-22 中，可以看到“生存时间（剩余）”显示为“00:00:53:12”，表示该 SA 的剩余有效时间为 53 分 12 秒。

2) 查看北京的 Netscreen

对于北京的 Netscreen 来说，可以通过命令 get sa 查看 IPSec 隧道的配置及状态信息，具体信息如下所示：

```
ns208-> get sa
total configured sa: 2
HEX ID   S/D Gateway          Port Algorithm      SPI         Life:sec kb Sta   PID vsys
00000025 0< 218.80.108.123     500 esp:3des/sha1 0xb9b84f1b  2717 4094M A/-    29 0
00000025 0> 218.80.108.123     500 esp:3des/sha1 0x115820fe  2717 4094M A/-    28 0
```

6.3.2 对方动态连接到本地

对方动态连接到本地是指要配置 HiPER VPN 网关作为 IPSec 隧道的响应方，一般具备静态的 IP 地址；IPSec 隧道的发起方往往不具备静态地址，可能是通过 DHCP 或者 PPPoE 等方式得到地址。本章讲述 HiPER 安全网关作为 IPSec 的响应方，同时对等方使用动态地址时的配置，采用野蛮模式进行协商。

6.3.2.1 HiPER 到 HiPER

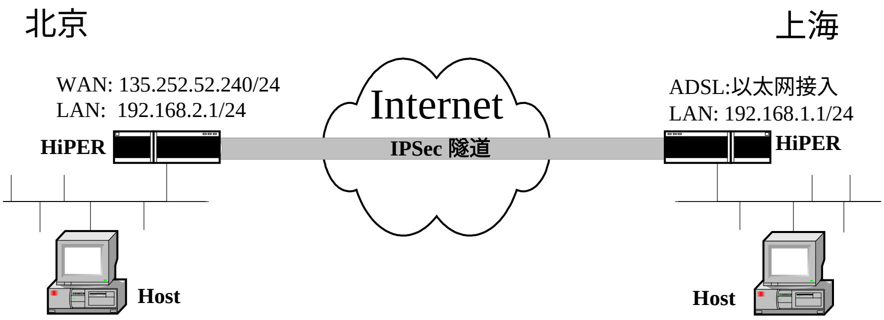


图 6-29 方案——HiPER 到 HiPER（对方动态连接到本地）

在本例中，如图 6-29 所示，通过使用带有预共享密钥的 IKE 协议，采用“自动”密钥方式在上海分公司和北京总部之间建立 IPSec 隧道，上海和北京的网关都使用 HiPER VPN 网关。上海的 HiPER VPN 网关通过以太网接入，以 DHCP 方式获得 IP 地址。对“第一阶段”和“第二阶段”安全级别的配置：“第一阶段”使用 HiPER 的缺省策略，“第二阶段”选择策略“esp-aes192-sha”。地址及预设参数如下：

上海的 HiPER：

WAN 口 IP 地址： 可变的，不确定

LAN 口 IP 地址： 192.168.1.1/24

认证用户名： hiper@utt.com.cn

预共享密钥： testing

北京的 HiPER：

WAN 口 IP 地址： 135.252.52.240/24

LAN 口 IP 地址： 192.168.2.1/24

1. 配置上海的 HiPER VPN 网关

在 ***VPN 配置—>IPSec*** 中，选择“添加”选项，然后在配置参数项中依次输入以下内容（没有列出的参数项无需配置），再单击“保存”按钮。

“设置名”：sh_bj

“设置方式”：自动

“自动方式”：动态连接到网关

“远端网关地址（名）”：135.252.52.240

“远端内网地址”：192.168.2.0

“本地绑定”：WAN1（eth2）

“本地内网地址”：192.168.1.0

“本地内网掩码”：255.255.255.0

“本地身份 ID”：hiper@utt.com.cn

“身份类型”：Email 地址

“预共享密钥”（安全选项）：testing

“加密认证算法 1”（安全选项）：esp-aes192-sha

高级选项中：

“协议”：任意

2. 配置北京的 HiPER VPN 网关

在 ***VPN 配置—>IPSec*** 中，选择“ 添加 ”选项，然后在配置参数项中依次输入以下内容（没有列出的参数项无需配置），再单击“ 保存 ”按钮。

“ 设置名 ”：bj_sh
“ 设置方式 ”：自动
“ 自动方式 ”：对方动态连接到本地
“ 远端网关地址 ”：0.0.0.0
“ 远端内网地址 ”：192.168.1.0
“ 远端内网掩码 ”：255.255.255.0
“ 远端身份 ID ”：hiper@utt.com.cn
“ 远端身份类型 ”：Email 地址
“ 本地绑定 ”：WAN1（eth2）
“ 本地内网地址 ”：192.168.2.0
“ 本地内网掩码 ”：255.255.255.0
“ 预共享密钥 ”（安全选项）：testing
“ 加密认证算法 1（安全选项）：esp-aes192-sha
高级选项中：
“ 协议 ”：任意

3. 查看状态

当双方配置完成后，上海和北京的 HiPER 通过流量或者手工触发建立起 IPSec 隧道。可以在 ***VPN 配置—>IPSec*** 中，查看“ IPSec 信息列表 ”，得到 IPSec 隧道的相关配置及状态信息。

1) 查看上海的 HiPER

如表 6-23、表 6-24、表 6-25 所示，为上海的 HiPER（使用动态 IP 地址）的 IPSec 隧道的相关信息。



IPSec 信息列表 1/16
1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

	设置名	设置方式	允许	SA状态	远端网关	远端内网地址	外出加密包个数	进入解密包个数	本地绑定
☐	sh_bj	自动	☑	已建立	135.252.52.240	192.168.2.0	10612	10679	eth2

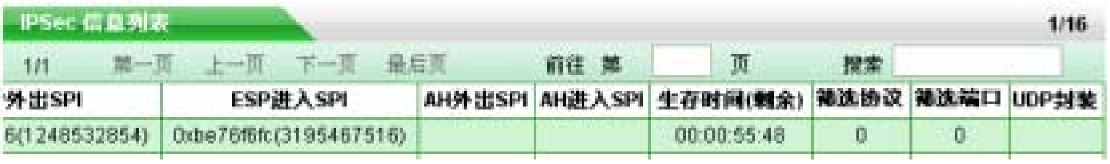
表 6-23 一方动态（HiPER 和 HiPER）— 发起方 IPSec 信息列表



IPSec 信息列表 1/16
1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

本地内网地址	协商模式	加密认证算法	ESP外出SPI	ESP进入SPI	AH外出SPI	AH
192.168.1.1	野蛮模式	esp-aes192-sha	0x4a6b1976(1248532854)	0xbe76f6fc(3195467516)		

表 6-24 一方动态（HiPER 和 HiPER）— 发起方 IPSec 信息列表（续表 6-23）



IPSec 信息列表 1/16
1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

外出SPI	ESP进入SPI	AH外出SPI	AH进入SPI	生存时间(剩余)	筛选协议	筛选端口	UDP封装
6(1248532854)	0xbe76f6fc(3195467516)			00:00:55:48	0	0	

表 6-25 一方动态（HiPER 和 HiPER）— 发起方 IPSec 信息列表（续表 6-24）

从表 6-23 中，可以看到“ 设置方式 ”显示为“ 自动 ”，“ SA 状态 ”显示为“ 已建立 ”，“ 外出加密包个数 ”和“ 进入解密包个数 ”均有数值显示，“ 本地绑定 ”显示为“ eth2 ”。

从表 6-24 中，可以看到“协商模式”显示为“野蛮模式”，“加密认证算法”显示为“esp-aes192-sha”，“ESP 外出 SPI”和“ESP 进入 SPI”显示为自动协商时得到的数值。

从表 6-25 中，可以看到“生存时间（剩余）”显示为“00:00:55:48”，表示该 SA 的剩余有效时间为 55 分 48 秒；“筛选协议”显示为“0”，表示对所有传输的数据包进行加密认证保护。

2) 查看北京的 HiPER

如表 6-26、表 6-27、表 6-28 所示，为北京的 HiPER（使用固定 IP 地址）的 IPSec 隧道的相关信息。

IPSec 信息列表 1/128

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

	设置名	设置方式	允许	SA状态	远端网关	远端内网地址	外出加密包个数	进入解密包个数	本地绑定	本
☐	bj_sh	自动	☑	已建立	135.252.52.1	192.168.1.0	10832	10765	eth2	1

表 6-26 一方动态（HiPER 和 HiPER）－响应方 IPSec 信息列表

IPSec 信息列表 1/128

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

本地内网地址	协商模式	加密认证算法	ESP外出SPI	ESP进入SPI	AH外出SPI	AH
192.168.2.0	野蛮模式	esp-aes192-sha	0xbe76f6fc(3195467516)	0x4a6b1976(1248532854)		

表 6-27 一方动态（HiPER 和 HiPER）－响应方 IPSec 信息列表（续表 6-26）

IPSec 信息列表 1/128

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

外出SPI	ESP进入SPI	AH外出SPI	AH进入SPI	生存时间(剩余)	筛选协议	筛选端口	UDP封装
3195467516)	0x4a6b1976(1248532854)			00:00:59:49	0	0	

表 6-28 一方动态（HiPER 和 HiPER）－响应方 IPSec 信息列表（续表 6-27）

从表 6-26 中，可以看到“设置方式”显示为“自动”，“SA 状态”显示为“已建立”，“远端网关”显示为“135.252.52.1”表示对端 HiPER 当前获得的地址为 135.252.52.1，“外出加密包个数”和“进入解密包个数” 均有数值显示，“本地绑定”显示为“eth2”。

从表 6-27 中，可以看到“协商模式”显示为“野蛮模式”，“加密认证算法”显示为“esp-aes192-sha”，“ESP 外出 SPI”和“ESP 进入 SPI”显示为自动协商时得到的数值。

从表 6-28 中，可以看到“生存时间（剩余）”显示为“00:00:59:49”，表示该 SA 的剩余有效时间为 59 分 49 秒；“筛选协议”显示为“0”，表示对所有传输的数据包进行加密认证保护。

6.3.3 动态连接到网关

动态连接到网关是指要配置的 HiPER 作为 IPSec 隧道的发起方，一般不具备静态的 IP 地址，可能是通过 DHCP 或者 PPPoE 等方式得到地址；IPSec 隧道的响应方往往具备静态地址。本章讲述 HiPER 作为 IPSec 的发起方并且对方是静态地址的配置，采用野蛮模式进行协商。

6.3.3.1 HiPER 到 HiPER

配置同章节 6.3.2.1（HiPER 到 HiPER）。

6.3.3.2 HiPER 到 Netscreen

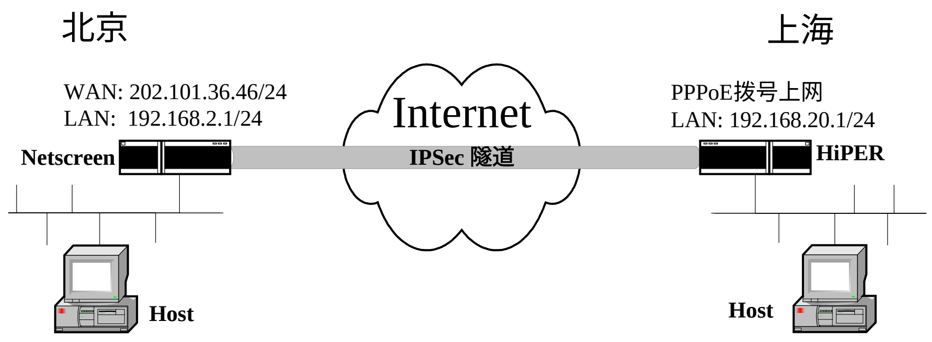


图 6-30 方案——HiPER 到 Netscreen（动态连接到网关）

在本例中，如图 6-30 所示，通过使用带有预共享密钥的 IKE 协议，采用 " 自动 " 密钥方式在上海分公司和北京总部之间建立 IPSec 隧道，在上海使用 HiPER VPN 网关，在北京使用 Netscreen。上海的 HiPER 通过 PPPoE 拨号上网，北京的 Netcreen 使用固定 IP 地址。双方均通过使用以 3DES 加密并经 SHA-1 认证的 ESP。地址及预设参数如下：

上海的 HiPER：

WAN 口 IP 地址： 可变的，不确定

LAN 口 IP 地址： 192.168.20.1/24

认证用户名： hipersh@abccompany.com

预共享密钥： h1i2p3e4r5

北京的 Netscreen：

ethernet3 口 IP 地址： 202.101.36.46/24

LAN 口 IP 地址： 192.168.2.1/24

1. 配置上海的 HiPER VPN 网关

在 ***VPN 配置—>IPSec*** 中，选择 " 添加 " 选项，然后在配置参数项中依次输入以下内容（没有列出的参数项无需配置），再单击 " 保存 " 按钮。

" 设置名 "：sh_to_bj

" 设置方式 "：自动

" 自动方式 "：动态连接到网关

" 远端网关地址（名）"：202.101.36.46

" 远端内网地址 "：192.168.2.0

" 远端内网掩码 "：255.255.255.0

" 本地绑定 "：PPPOE

" 本地内网地址 "：192.168.20.0

" 本地内网掩码 "：255.255.255.0

" 本地身份 ID "：hipersh@abccompany.com

" 本地身份类型 "：Email 地址

" 预共享密钥 "（安全选项）：h1i2p3e4r5

“加密认证算法 1”（安全选项）：esp-3des-sha

2. 配置北京的 Netscreen

这里只给出基于 WEB UI 方式下配置 Netscreen 的方法。

配置接口－安全区段

1） 进入“Network”→“Interfaces”，单击“ethernet7 ”后的“Edit”超链接，输入以下内容，然后单击“OK”按钮。

“Zone Name”：Trust

“IP Address/Netmask”：192.168.2.1/24

2） 进入“Network”→“Interfaces”，单击“ethernet3”后的“Edit”超链接，输入以下内容，然后单击“OK”按钮。

“Zone Name”：Untrust

“IP Address/Netmask”：202.101.36.46/24

配置地址

3） 进入“Objects”→“Addresses”→“ List”，单击“New”按钮，再输入以下内容，然后单击“OK”按钮。

“Address Name”：Trust_LAN

“IP Address/Domain Name”：选中“IP/Netmask”

“IP/Netmask”：192.168.2.0/24

“Zone”：Trust

4） 进入“Objects”→“Addresses”→“ List”，单击“New”按钮，再输入以下内容，然后单击“OK”按钮。

“Address Name”：sh_office

“IP Address/Domain Name”：选中“IP/Netmask”

“IP/Netmask”：192.168.20.0/24

“Zone”：Untrust

配置 VPN

5） 进入“VPNs”→“AutoKey Advanced”→“Gateway”，单击“New”按钮，再输入以下内容。

“Gateway Name”：To_shanghai

“Security Level”：Custom

“Remote Gateway Type”：选中“Dynamic IP Address”

“Peer ID”：hipersh@abccompany.com

“Preshared Key”：h1i2p3e4r5

“Outgoing Interface”：ethernet3

单击“Advanced”按钮，再输入以下高级设置参数：

“Security Level”：Custom

“Phase 1 Proposal（For Custom Security Level）”：pre-g2-3des-sha

“Mode（Initiator）”：Aggressive

“Outgoing Interface”：ethernet3

然后单击“Return”按钮，返回到上一页，再单击“OK”按钮。

6） 进入“VPNs”→“AutoKey IKE”，单击“New”按钮，再输入以下内容，然后单击“OK”按钮。

“VPN Name”：corp_branch

“ Security Level ”：Compatible
“ Remote Gateway ”：选中 “ Predefined ”
“ Predefined ”：to_shanghai

配置路由

7） 进入 “ Network ” → “ Routing ” → “ Routing Table ”，选中 “ trust-vr ”，单击 “ New ” 按钮，再输入以下内容，然后单击 “ OK ” 按钮。
“ Network Address/Netmask ”：0.0.0.0/0
“ Gateway ”：选中
“ Interface ”：ethernet3（untrust）
“ Gateway IP Address ”：202.101.36.1

配置策略

8） 进入 “ Policies ”，“ From ” 选中 “ DMZ ”，“ To ” 选中 “ Untrust ”，单击 “ New ” 按钮，再输入以下内容，然后单击 “ OK ” 按钮。
“ Source Address ”：选中 “ Address Book ”
“ Address Book ”：Trust_LAN
“ Destination Address ”：选中 “ Address Book ”
“ Address Book ”：sh_office
“ Service ”：ANY
“ Action ”：Tunnel
“ VPN Tunnel ”：corp _branch
“ Modify matching VPN policy ”：选中
“ Position at Top ”：选中

3. 查看状态

当双方配置完成后，上海的 HiPER 和北京的 Netscreen 通过流量或者手工触发建立起 IPSec 隧道。

1) 查看上海的 HiPER

对于上海的 HiPER 来说，可以在 ***VPN 配置—>IPSec*** 中，查看 “ IPSec 信息列表 ”，得到 IPSec 隧道的相关配置及状态信息，如表 6-29、表 6-30、表 6-31 所示。


IPSec 信息列表　1/16
1/1　第一页　上一页　下一页　最后页　前往 第 页　搜索

	设置名	设置方式	允许	SA状态	远端网关	远端内网地址	外出加密包个数	进入解密包个数	本地绑定
☐	sh_to_bj	自动	☑	已建立	202.101.36.46	192.168.2.0	1941	1941	PPPOE

表 6-29 HiPER 动态（HiPER 和 Netsceen）－IPSec 信息列表


IPSec 信息列表　1/16
1/1　第一页　上一页　下一页　最后页　前往 第 页　搜索

本地内网地址	协商模式	加密认证算法	ESP外出SPI	ESP进入SPI	AH外出SPI	AH进入
192.168.20.1	野蛮模式	esp-3des-sha	0x115820fd(290988285)	0xb9b84f1a(3115863834)		

表 6-30 HiPER 动态（HiPER 和 Netsceen）－IPSec 信息列表（续表 6-29）

IPSec 信息列表 1/16

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

外出SPI	ESP进入SPI	AH外出SPI	AH进入SPI	生存时间(剩余)	筛选协议	筛选端口	UDP封装
(290988285)	0xb9b84f1a(3115863834)			00:00:50:09	0	0	

表 6-31 HiPER 动态（HiPER 和 Netsceen）－IPSec 信息列表（续表 6-30）

从表 6-29 中，可以看到“ 设置方式 ”显示为“ 自动 ”,“ SA 状态 ”显示为“ 已建立 ”,“ 外出加密包个数 ”和“ 进入解密包个数 ” 均有数值显示。

从表 6-30 中，可以看到“ 本地绑定 ”显示为“ PPPOE ”,“ 协商模式 ”显示为“ 野蛮模式 ”,“ 加密认证算法 ”显示为“ esp-3des-sha ”,“ ESP 外出 SPI ”和“ ESP 进入 SPI ”显示为自动协商时得到的数值。

从表 6-31 中，可以看到“ 生存时间（剩余）”显示为“ 00:00:50:09 ”，表示该 SA 的剩余有效时间为 50 分 09 秒。

2) 查看北京的 Netscreen

对于北京的 Netscreen 来说，可以通过命令 get sa 查看 IPSec 隧道的配置及状态信息，具体信息如下所示：

```
ns208-> get sa
total configured sa: 9
HEX ID    S/D Gateway        Port Algorithm     SPI        Life:sec kb Sta    PID vsys
0000001a 0< 218.80.150.39    500 esp:3des/sha1 0xb9b84f1a  3224 4095M A/-    21 0
0000001a 0> 218.80.150.39    500 esp:3des/sha10x115820fd   3224 4095M A/-    20 0
```

6.3.3.3 HiPER 到 Fortigate

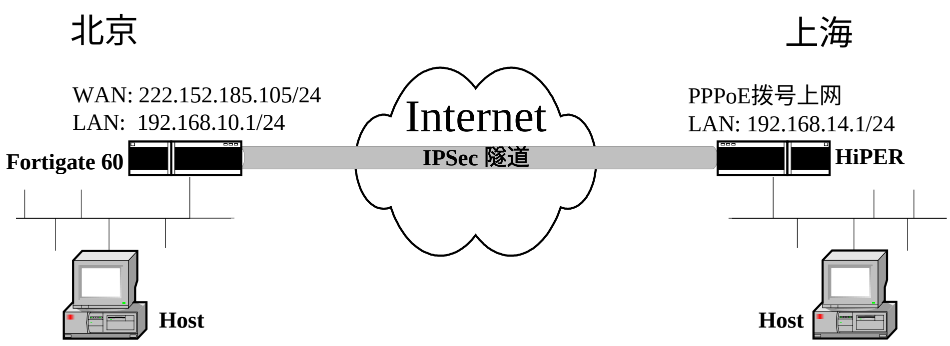


图 6-31 方案——HiPER 到 Fortigate（动态连接到网关）

在本例中，如图 6-31 所示，通过使用带有预共享密钥的 IKE 协议，采用“ 自动 ”方式在上海分公司和北京总部之间建立 IPSec 隧道。在上海使用 HiPER VPN 网关，通过 PPPoE 拨号上网；在北京使用 Fortigate 60，具有固定 IP 地址。双方均通过使用以 AES192 加密并经 SHA-1 认证的 ESP。地址及预设参数如下：

上海的 HiPER：

WAN 口 IP 地址： 可变的，不确定

LAN 口 IP 地址： 192.168.14.1/24

认证用户名： hipersh@abccompany.com

预共享密钥： testing

北京的 Netscreen：

WAN1 口 IP 地址： 222.152.185.105/24
LAN 口 IP 地址： 192.168.10.1/24

1. 配置上海的 HiPER VPN 网关

在 ***VPN 配置—>IPSeC*** 中，选择“ 添加 ”选项，然后在配置参数项中依次输入以下内容（没有列出的参数项无需配置），再单击“ 保存 ”按钮。

“ 设置名 ”：to_bj
“ 设置方式 ”：自动
“ 自动方式 ”：动态连接到网关
“ 远端网关地址（名）”：222.152.185.105
“ 远端内网地址 ”：192.168.10.0
“ 远端内网掩码 ”：255.255.255.0
“ 本地绑定 ”：PPPoE
“ 本地内网地址 ”：192.168.14.0
“ 本地内网掩码 ”：255.255.255.0
“ 本地身份 ID ”：hipersh@abccompany.com
“ 本地身份类型 ”：Email 地址
“ 预共享密钥 ”（安全选项）：testing
“ 加密认证算法 1 ”（安全选项）：esp-aes192-sha
高级选项中：
“ 协商模式 ”：野蛮模式
“ DPD ”：选中

2. 配置北京的 Fortigate

这里只给出基于 WEB UI 方式下配置 Fortigate 的方法。

配置端口地址

1） 进入“ 系统管理 ”→“ 网络 ”→“ 接口 ”，单击“ port1 ”后的编辑按钮，在“ IP 地址/网络掩码 ”中输入“ 192.168.10.1/255.255.255.0 ”，再单击“ OK ”按钮；
2） 进入“ 系统管理 ”→“ 网络 ”→“ 接口 ”，单击“ port6 ”后的编辑按钮，在“ IP 地址/网络掩码 ”中输入“ 222.152.185.105/255.255.255.0 ”，再单击“ OK ”按钮；

配置地址和地址组

3） 进入“ 防火墙 ”→“ 地址 ”→“ 地址 ”，单击“ 新建 ”按钮，在地址名称中输入“ local ”，在“ 子网/IP 范围 ”中输入“ 192.168.10.1/255.255.255.0 ”，再单击“ OK ”按钮；
4） 进入“ 防火墙 ”→“ 地址 ”→“ 地址 ”，单击“ 新建 ”按钮，在地址名称中输入“ remote ”，在“ 子网/IP 范围 ”中输入“ 192.168.14.0/255.255.255.0 ”，再单击“ OK ”按钮；

配置 IPSec 协商参数

5） 第一阶段

进入“ 虚拟专网 ”→“ IPSEC ”，单击“ 创建阶段 1 ”按钮，在配置参数中依次输入（或选择）以下内容，再单击“ OK ”按钮。

“ 网关名称 ”：sh_branch
“ 远程网关 ”： 连接用户
“ 模式 ”：野蛮模式
“ 阶段 1 交互计划 ” 中的 “ 1-加密算法 ”：3DES ;“ 认证 ”：SHA1

"DH 组"：2
"密钥周期"：28800
"认证方式"： 预共享密钥
"预共享密钥"：testing
高级选项中：
"对等体选项"：接收此对等体 ID
"接受此对等体"：hipersh@abccompany.com
"Xauth"：禁用
"NAT 穿越"：不选

6） 第二阶段

进入"虚拟专网"→"IPSEC"单击"创建阶段 2"按钮，在配置参数中依次输入（或选择）以下内容，再单击"OK"按钮。

"通道名称"：bj_sh
"远程网关"：sh_branch
"阶段 2 交互计划"中，
"1-加密算法"：AES192 ；"认证算法"：SHA1
"启用数据重演检测"：不选
"启用完全转发安全性(PFS)"：不选
"密钥周期"：1800 秒
"保持存活"： 启用

配置加密策略

7） internal 到 wan1

进入"防火墙"→"策略"，单击"Create New"按钮，在配置参数中依次输入（或选择）以下内容，再单击"OK"按钮。

"源接口/区"：port1
"源地址"： local
"目的接口/区"：port6
"目的地址"：remote
"时间表"：Always
"服务"：ANY
"模式"：IPSEC
"VPN 通道"：sh_branch

3. 查看状态

当双方配置完成后，上海的 HiPER 和北京的 Fortigate 通过流量或者手工触发建立起 IPSec 隧道。

1) 查看上海的 HiPER

对于上海的 HiPER 来说，可以在 ***VPN 配置—>IPSec*** 中，查看"IPSec 信息列表"，得到 IPSec 隧道的相关配置及状态信息，如表 6-32、表 6-33、表 6-34 所示。

IPSec 信息列表 1/16

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

	设置名	设置方式	允许	SA状态	远端网关	远端内网地址	外出加密包个数	进入解密包个数	本地绑定
☐	to_bj	自动	☑	已建立	222.152.185.105	192.168.10.1	2380	2380	PPPOE

表 6-32 HiPER 动态（HiPER 和 Fortigate）－IPSec 信息列表

IPSec 信息列表 1/16

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

本地内网地址	协商模式	加密认证算法	ESP外出SPI	ESP进入SPI	AH外出SPI	AH进
192.168.14.1	野蛮模式	esp-aes192-sha	0xe5812f41(3850448705)	0xf1358866(4046817382)		

表 6-33 HiPER 动态（HiPER 和 Fortigate）－IPSec 信息列表（续表 6-32）

IPSec 信息列表 1/16

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

P外出SPI	ESP进入SPI	AH外出SPI	AH进入SPI	生存时间(剩余)	筛选协议	筛选端口	UDP封装
1(3850448705)	0xf1358866(4046817382)			00:00:45:18	0	0	

表 6-34 HiPER 动态（HiPER 和 Fortigate）－IPSec 信息列表（续表 6-33）

从表 6-32 中，可以看到“设置方式”显示为“自动”，“SA 状态”显示为“已建立”，“外出加密包个数”和“进入解密包个数”均有数值显示，“本地绑定”显示为“PPPOE”。

从表 6-33 中，可以看“协商模式”显示为“野蛮模式”，“加密认证算法”显示为“esp-aes192-sha”，“ESP 外出 SPI”和“ESP 进入 SPI”显示为自动协商时得到的数值。

从表 6-34 中，可以看到“生存时间（剩余）”显示为“00:00:45:18”，表示该 SA 的剩余有效时间为 45 分 18 秒。

2) 查看北京的 Fortigate

对于北京的 Fortigate 来说，进入“虚拟专网”→“IPSEC”→“动态 VPN 监视器”中，可查看相关连接信息，如表 6-35 所示。

名称	远程往关	用户名	超时
sh_branch_0	10.10.10.15:0	hipersh@abccompany.com	1402

超时	代理ID来源	代理ID目的	
1402	192.168.10.*	192.168.14.*	

表 6-35 IPSec 隧道连接状态

6.4 HiPER 的 IPSec 的综合应用

6.4.1 NAT 穿透——HiPER 和 Netscreen

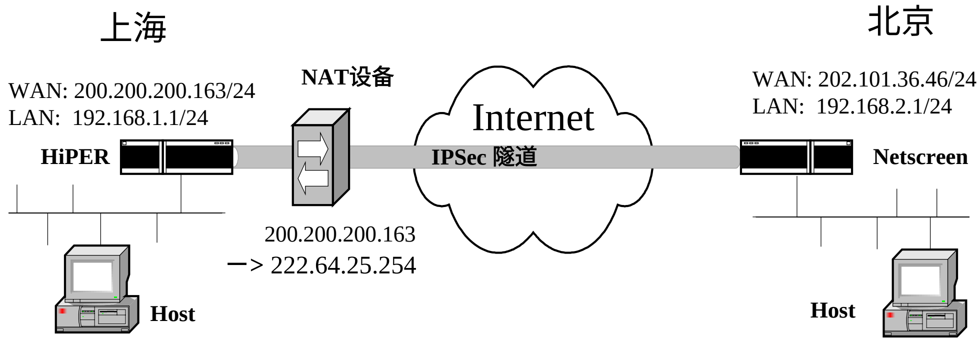


图 6-32 方案——NAT 穿透（HiPER 和 Netscreen）

在本例中，如图 6-32 所示，通过使用带有预共享密钥的 IKE 协议，采用“自动”密钥方式在上海分公司和北京总部之间建立 IPSec 隧道，在北京使用 Netscreen；在上海使用 HiPER VPN 网关。在上海，HiPER 通过一个 NAT 设备连到公共网络，它将所有来自 HiPER 的数据包的外部包头中的初始 IP 源地址（200.200.200.163）替换成新地址 222.64.25.254。在第一阶段协商过程中，隧道两端设备（HiPER 和 Netscreen）将检测双方均否都支持 NAT-T，NAT 是否沿着数据路径出现。地址及预设参数如下：

上海的 HiPER：

WAN 口： 200.200.200.163/24

静态网关：200.200.200.254/24

LAN 口： 192.168.1.1/24

北京的 Netscreen：

ethernet3 口： 202.101.36.46/24

静态网关：202.101.36.1/24

LAN 口： 192.168.2.1/24

1. 配置上海的 HiPER VPN 网关

提示：由于 Netscreen 中，用来进行 NAT 穿透的 UDP 封包的端口号为 500，因此在本例中，须将“NAT 穿透”的参数“端口”配置成 500。

在 ***VPN 配置—>IPSec*** 中，选择“添加”选项，然后在配置参数项中依次输入以下内容（没有列出的参数项无需配置），再单击“保存”按钮。

“设置名”：to_bj

“设置方式”：自动

“自动方式”：动态连接到网关

“远端网关地址（名）”：202.101.36.46

“远端内网地址”：192.168.2.0

“远端内网掩码”：255.255.255.0

“本地绑定”：WAN（eth2）

"本地内网地址"：192.168.1.0
"本地内网掩码"：255.255.255.0
"本地身份 ID"：hipersh@abccompany.com
"本地身份类型"：Email 地址
"预共享密钥"（安全选项）：h1i2p3e4r5
"加密认证算法 1"（安全选项）：esp-aes128-sha
高级选项中：
"协商模式"：野蛮模式
"DPD"：选中
"NAT 穿透"：选中
"端口"：500
"维持"：20

2. 配置北京的 Netcreen
这里只给出基于 WEB UI 方式下配置 Netscreen 的方法。

配置接口－安全区段

1） 进入"Network"→"Interfaces"，单击"ethernet7 "后的"Edit"超链接，输入以下内容，然后单击"OK"按钮。
"Zone Name"：Trust
"IP Address/Netmask"：192.168.2.1/24
2） 进入"Network"→"Interfaces"，单击"ethernet3"后的"Edit"超链接，输入以下内容，然后单击"OK"按钮。
"Zone Name"：Untrust
"IP Address/Netmask"：202.101.36.46/24

配置地址

3） 进入"Objects"→"Addresses"→" List"，单击"New"按钮，再输入以下内容，然后单击"OK"按钮。
"Address Name"：Trust_lan
"IP Address/Domain Name"：选中"IP/Netmask"
"IP/Netmask"：192.168.2.0/24
"Zone"：Trust
4） 进入"Objects"→"Addresses"→" List"，单击"New"按钮，再输入以下内容，然后单击"OK"按钮。
"Address Name"：sh_office
"IP Address/Domain Name"：选中"IP/Netmask"
"IP/Netmask"：192.168.1.0/24
"Zone"：Untrust

配置 VPN

5） 进入"VPNs"→"AutoKey Advanced"→"Gateway"，单击"New"按钮，再输入以下内容，然后单击"OK"按钮。
"Gateway Name"：To_shanghai
"Security Level"：Custom
"Remote Gateway Type"：选中"Dynamic IP Address"

"Peer ID"：hipersh@abccompany.com
"Preshared Key"：h1i2p3e4r5
"Outgoing Interface"：ethernet3
再单击"Advanced"按钮，输入以下高级设置参数：
"Security Level"：Custom
"Phase 1 Proposal"：pre-g2-3des-sha
"Mode（Initiator）"：Aggressive
"Enable NAT-Traversal"：选中
"Keepalive Frequency"：20
然后单击"Return"按钮，返回到上一页，再单击"OK"按钮。

6） 进入"VPNs"→"AutoKey IKE"，单击"New"按钮，再输入以下内容。
"VPN Name"：corp_branch
"Security Level"：Custom
"Remote Gateway"：选中"Predefined"
"Predefined"：to_shanghai
再单击"Advanced"按钮，在"Phase 2 Proposal"中选择"nopfs-esp-aes128-sha"，然后单击"Return"按钮，返回到上一页，再单击"OK"按钮。

配置路由

7） 进入"Network"→"Routing"→"Routing Table"，选中"trust-vr"，单击"New"按钮，再输入以下内容，然后单击"OK"按钮。
"Network Address/Netmask"：0.0.0.0/0
"Gateway"：选中
"Interface"：ethernet3（untrust）
"Gateway IP Address"：202.101.36.1

配置策略

8） 进入"Policies"，"From"选中"DMZ"，"To"选中"Untrust"，单击"New"按钮，再输入以下内容，然后单击"OK"按钮。
"Source Address"：选中"Address Book"
"Address Book"：Trust_LAN
"Destination Address"：选中"Address Book"
"Address Book"：sh_office
"Service"：ANY
"Action"：Tunnel
"VPN Tunnel"：corp _branch
"Modify matching VPN policy"：选中
"Position at Top"：选中

3. 查看状态

当双方配置完成后，上海的 HiPER 和北京的 Netscreen 通过流量或者手工触发建立起 IPSec 隧道。

1) 查看上海的 HiPER

对于上海的 HiPER 来说，可以在 ***VPN 配置—>IPSec*** 中，查看"IPSec 信息列表"，得到 IPSec 隧道的相关配置及状态信息，如表 6-36、表 6-37、表 6-38 所示。

IPSec 信息列表　1/16

1/1　第一页　上一页　下一页　最后页　前往 第　页　搜索

	设置名	设置方式	允许	SA状态	远端网关	远端内网地址	外出加密包个数	进入解密包个数	本地绑定	本
☐	to_bj	自动	☑	已建立	202.101.36.46	192.168.2.1	1762	1762	eth2	

表 6-36 NAT 穿透（HiPER 和 Netsceen）－IPSec 信息列表

IPSec 信息列表　1/16

1/1　第一页　上一页　下一页　最后页　前往 第　页　搜索

本地内网地址	协商模式	加密认证算法	ESP外出SPI	ESP进入SPI	AH外出SPI	AH
192.168.1.1	野蛮模式	esp-aes128-sha	0xbf4431cf(3208917455)	0x5de8792c(1575516460)		

表 6-37 NAT 穿透（HiPER 和 Netsceen）－IPSec 信息列表（续表 6-36）

IPSec 信息列表　1/16

1/1　第一页　上一页　下一页　最后页　前往 第　页　搜索

外出SPI	ESP进入SPI	AH外出SPI	AH进入SPI	生存时间(剩余)	筛选协议	筛选端口	UDP封装
3208917455)	0x5de8792c(1575516460)			00:00:50:45	0	0	

表 6-38 NAT 穿透（HiPER 和 Netsceen）－IPSec 信息列表（续表 6-37）

从表 6-36 中，可以看到“设置方式”显示为“自动”，“SA 状态”显示为“已建立”，“外出加密包个数”和“进入解密包个数”均有数值显示，可以看到“本地绑定”显示为“eth2”。

从表 6-37 中，可以看到“协商模式”显示为“野蛮模式”，“加密认证算法”显示为“esp-aes128-sha”，“ESP 外出 SPI”和“ESP 进入 SPI”显示为自动协商时得到的数值。

从表 6-38 中，可以看到“生存时间（剩余）”显示为“00:00:50:45”，表示该 SA 的剩余有效时间为 50 分 45 秒。

2) 查看北京的 Netscreen

对于北京的 Netscreen 来说，可以通过命令 get sa 查看 IPSec 隧道的配置及状态信息，具体信息如下所示：

```
ns208-> get sa
total configured sa: 9
HEX ID    S/D Gateway          Port Algorithm        SPI          Life:sec kb Sta     PID vsys
00000025 0< 222.64.25.254   18328 esp:a128/sha1 0xbf4431cf   3294 4093M A/-      29 0
00000025 0> 222.64.25.254   18328 esp:a128/sha1 0x5de8792c   3294 4093M A/-      28 0
```

6.4.2 L2TP over IPSec ——HiPER 和 Cisco

由于 L2TP 构建的 VPN 隧道不够安全，而 IPSec 在一些情况下不能通过一些网络设备，比如 NAT，及其他防火墙，因此可以考虑把二者结合起来使用。L2TP 和 IPSec 相结合后称为 L2TP/IPSec，这是一种安全性极高的技术，用于通过公共网络（如 Internet）建立远程访问虚拟专用网络（VPN）连接。

L2TP/IPSec 有两种使用形式，即 L2TP over IPSec 和 IPSec over L2TP，两种方式的对比如表 6-39 所示。

方式 特征	L2TP over IPSec	IPSec over L2TP
隧道建立顺序	先建立 IPSec 隧道，再建立 L2TP 隧道	先建立 L2TP 隧道，再建立 IPSec 隧道
协议栈顺序	L2TP 位于 IPSec 上面	IPSec 位于 L2TP 上面
包封装顺序	先封装 L2TP，再封装 IPSec	先封装 IPSec，再封装 L2TP
IPSec 加密对象	对 L2TP 封装后的整个数据包加密	仅对用户数据加密，不对 L2TP 封装信息加密
能否通过 NAT 或其他防火墙	不一定	能够
L2TP 隧道两端地址	内网地址	内网地址
IPSec 隧道两端地址	外网地址	内网地址

表 6-39 L2TP over IPSec 与 IPSec over L2TP 之比较

本节主要介绍 L2TP over IPSec 的应用实例，在本例中，如图 6-33 所示，通过使用带有预共享密钥的 IKE 协议，采用“ 自动 ”密钥方式在上海分公司和北京总部之间采用 L2TP over IPSec 方式建立 VPN 隧道。上海使用 HiPER VPN 网关作为 L2TP 客户端，同时使其作为 IPSec 隧道的一端；北京使用 Cisco 2611 作为 L2TP 服务器，同时使其作为 IPSec 隧道的另一端。

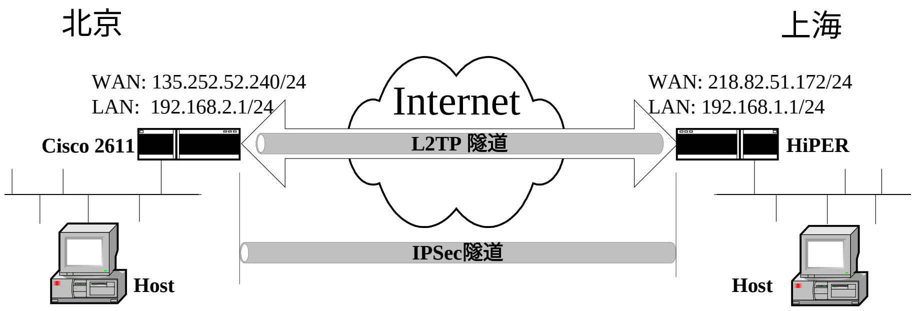


图 6-33 方案 L2TP over IPSec（HiPER 和 Cisco）

地址如下：

上海的 HiPER：

WAN 口： 218.82.51.172/24

静态网关：218.82.51.1/24

LAN 口： 192.168.1.1/24

北京的 Cisco 2611：

fastethernet0/0 口（外网接口）： 135.252.52.240/24

静态网关：135.252.52.1/24

fastethernet0/1 口（内网接口）： 192.168.2.1/24

1. 配置上海的 HiPER VPN 网关

提示：由于在 L2TP over IPSec 方式下，是由 L2TP 触发 IPSec 协商，也就是说 IPSec 加密的对象是 L2TP 数据包，因此在为 HiPER 配置 IPSec 隧道参数时，“ 远端内网地址 ” 和 “ 本地内网地址 ” 这两个参数均应配置成 L2TP 隧道的终结地址。本例中，IPSec 隧道起始于 135.252.52.240，即 Cisco 2611 的 fastethernet0/0 口地址；终止于 218.82.51.172，即 HiPER

的 WAN 口地址。

1) 配置 HiPER 成为 L2TP 客户端

在 ***VPN 配置—>PPTP/L2TP*** 中，选择 “ 添加 ” 选项，然后在配置参数项中依次输入以下内容（没有列出的参数项无需配置），再单击 “ 保存 ” 按钮。

“ 设置名 ”：l2tp_ipsec
“ 业务类型 ”：拨出（客户端）
“ 用户名 ”：l2tp
“ 协议类型 ”：L2TP
“ 密码 ”：test
“ 确认密码 ”：test
“ 密码验证方式 ”：CHAP
“ 远端内网 IP 地址 ”：192.168.2.0
“ 远端内网子网掩码 ”：255.255.255.0
“ 隧道服务器地址 ”：135.252.52.240

2) 配置 IPSec 隧道参数

在 ***VPN 配置—>IPSec*** 中，选择 “ 添加 ” 选项，然后在配置参数项中依次输入以下内容（没有列出的参数项无需配置），再单击 “ 保存 ” 按钮。

“ 设置名 ”：l2tpoipsec
“ 设置方式 ”：自动
“ 自动方式 ”：网关到网关
“ 远端网关地址（名）”：135.252.52.240
“ 远端内网地址 ”：135.252.52.240
“ 远端内网掩码 ”：255.255.255. 255
“ 本地绑定 ”：WAN1（eth2）
“ 本地内网地址 ”：218.82.51.172
“ 本地内网掩码 ”：255.255.255.255
“ 预共享密钥 ”（安全选项）：test
“ 加密认证算法 1 ”（安全选项）：esp-des
高级选项中：
“ 协议 ”（筛选条件）：UDP
“ 端口 ”（筛选条件）：1701
“ 协商模式 ”：主模式

2. 配置北京的 Cisco 2611 路由器

Cisco 2611 路由器只支持 CLI 方式，具体配置如下：

//配置 L2TP 用户名、口令

username l2tp password 0 testing

//激活 vpdn

vpdn enable

//配置 vpdn 组 1

vpdn-group 1
! Default L2TP VPDN group
accept-dialin

protocol l2tp

virtual-template 1

local name cisco

lcp renegotiation always

no l2tp tunnel authentication

//配置第一阶段安全策略

crypto isakmp policy 1

authentication pre-share

group 2

//配置预共享密钥

crypto isakmp key testing address 218.82.51.172

//配置第二阶段加密认证算法

crypto ipsec transform-set 1set esp-des

//配置第二阶段安全策略

crypto map l2tpoveripsec 10 ipsec-isakmp

set peer 218.82.51.172

set transform-set 1set

match address 101

//配置外网接口

interface FastEthernet0/0

ip address 135.252.52.240 255.255.255.0

//将安全策略绑定到外网端口

crypto map l2tpoveripsec

//配置内网接口

interface FastEthernet0/1

ip address 192.168.2.1 255.255.255.0

//配置 L2TP 的虚拟模板

!interface Virtual-Template1

ip unnumbered FastEthernet0/1

peer default ip address pool l2tppool

ppp authentication chap

//配置 L2TP 拨号用户的地址池

ip local pool l2tppool 200.1.1.1

ip classless

//配置静态路由

ip route 0.0.0.0 0.0.0.0 135.252.52.1

ip route 192.168.1.0 255.255.255.0 200.1.1.1

//配置 ACL 表，在第二阶段安全策略中引用

access-list 101 permit udp host 135.252.52.240 eq 1701 host 218.82.51.172 eq 1701

3. 查看状态

当双方配置完成后，上海的 HiPER 和北京的 Cisco 通过流量或者手工触发建立起 VPN 隧道。

1) 查看上海的 HiPER

对于上海的 HiPER 来说，可以在 ***VPN 配置—>PPTP 和 L2TP*** 中，查看 “ PPTP/L2TP 信息列表 ”，得到 L2TP 隧道的相关配置及状态信息，如表 6-40、表 6-41 所示；同时可以在 ***VPN 配置—>IPSec*** 中，查看 “ IPSec 信息列表 ”，得到 IPSec 隧道的相关配置及状态信息，如表 6-42、表 6-43、表 6-44 所示。

PPTP/L2TP 信息列表 1/17

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

	设置名	用户名	允许	会话状态	远端网关	远端内网地址	使用时间
☐	l2tp_ipsec	l2tp	☑	已连接	135.252.52.240	192.168.2.0	00:00:16:01

表 6-40 L2TP over IPSec with Cisco — L2TP 信息列表

PPTP/L2TP 信息列表 1/17

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

使用时间	空闲时间	出流量	入流量	业务类型	协议类型	虚接口地址	是否加密
00:00:17:43	00:00:00:01	108666	107994	VPN拨出	L2TP	200.1.1.1	否

表 6-41 L2TP over IPSec with Cisco — L2TP 信息列表（续表 6-40）

从表 6-40 中，可以看到 “ 会话状态 ” 显示为 “ 已连接 ”, “ 出流量 ” 和 “ 入流量 ” 中均有数值显示；

从表 6-41 中，可以看到 “ 业务类型 ” 显示为 “ VPN 拨出 ”，协议类型显示为 “ L2TP ”，是否加密显示为 “ 否 ”。

IPSec 信息列表 1/16

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

	设置名	设置方式	允许	SA状态	远端网关	远端内网地址	外出加密包个数	进入解密包个数	本地绑
☐	l2tpoipsec	自动	☑	已建立	135.252.52.240	135.252.52.240	1328	1316	eth2

表 6-42 L2TP over IPSec with Cisco — IPSec 信息列表

IPSec 信息列表 1/16

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

本地绑定	本地内网地址	协商模式	加密认证算法	ESP外出SPI	ESP进入SPI	AH外出S
eth2	218.82.51.172	主模式	esp-des	0x863987da(2251917274)	0x40f05b89(1089493897)	

表 6-43 L2TP over IPSec with Cisco — IPSec 信息列表（续表 6-42）

IPSec 信息列表 1/16

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

P外出SPI	ESP进入SPI	AH外出SPI	AH进入SPI	生存时间(剩余)	筛选协议	筛选端口	UDP封装
da(2251917274)	0x40f05b89(1089493897)			00:00:43:16	17	1701	

表 6-44 L2TP over IPSec with Cisco — IPSec 信息列表（续表 6-43）

从表 6-42 中，可以看到“ 设置方式 ”显示为“ 自动 ”, “ SA 状态 ”显示为“ 已建立 ”， “ 外出加密包个数 ” 和 “ 进入解密包个数 ” 均有数值显示。

从表 6-43 中，可以看到 “ 本地绑定 ” 显示为 “ eth2 ”, “ 协商模式 ” 显示为 “ 主模式 ”, “ 加密认证算法 ” 显示为 “ esp-des ”, “ ESP 外出 SPI ” 和 “ ESP 进入 SPI ” 显示为自动协商时得到的数值。

从表 6-44 中，可以看到 “ 生存时间（剩余）” 显示为 “ 00:00:43:16 ”，表示该 SA 的剩余有效时间为 43 分 16 秒。

2) 查看北京的 Cisco

对于 Cisco 2611 路由器来说，可以通过命令 show crypto ipsec sa 、show vpdn session 及 show vpdn tunnel 查看 VPN 隧道配置及状态信息，具体信息如下：

```
Router#show crypto ipsec sa
interface: FastEthernet0/0
    Crypto map tag: l2tpoveripsec, local addr. 135.252.52.240
   local  ident (addr/mask/prot/port): (135.252.52.240/255.255.255.255/17/1701)
   remote ident (addr/mask/prot/port): (218.82.51.172/255.255.255.255/17/1701)
   current_peer: 218.82.51.172
     PERMIT, flags={origin_is_acl,reassembly_needed,parent_is_transport,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0
     local crypto endpt.: 135.252.52.240, remote crypto endpt.: 218.82.51.172
     path mtu 1500, ip mtu 1500
     current outbound spi: 0
     inbound esp sas:
     inbound ah sas:
     inbound pcp sas:
     outbound esp sas:
     outbound ah sas:
     outbound pcp sas:
   local  ident (addr/mask/prot/port): (135.252.52.240/255.255.255.255/17/1701)
   remote ident (addr/mask/prot/port): (218.82.51.172/255.255.255.255/17/1701)
   current_peer: 218.82.51.172
     PERMIT, flags={reassembly_needed,}
    #pkts encaps: 16424, #pkts encrypt: 16424, #pkts digest 0
    #pkts decaps: 26886, #pkts decrypt: 26886, #pkts verify 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0
     local crypto endpt.: 135.252.52.240, remote crypto endpt.: 218.82.51.172
     path mtu 1500, ip mtu 1500      current outbound spi: 1925811C
     inbound esp sas:
      spi: 0xEB88D4C4(3951613124)
        transform: esp-des ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2002, flow_id: 3, crypto map: l2tpoveripsec
        sa timing: remaining key lifetime (k/sec): (4194297/2497)
        IV size: 8 bytes
        replay detection support: N
      spi: 0x4BC16573(1270965619)
        transform: esp-des ,
```

```
      in use settings ={Tunnel, }
      slot: 0, conn id: 2006, flow_id: 7, crypto map: l2tpoveripsec
      sa timing: remaining key lifetime (k/sec): (4194298/2516)
      IV size: 8 bytes
      replay detection support: N
   spi: 0x4D29B2D5(1294578389)
      transform: esp-des ,
      in use settings ={Tunnel, }
      slot: 0, conn id: 2008, flow_id: 9, crypto map: l2tpoveripsec
      sa timing: remaining key lifetime (k/sec): (4194298/2545)
      IV size: 8 bytes
      replay detection support: N
   spi: 0x31C3DB94(834919316)
      transform: esp-des ,
      in use settings ={Tunnel, }
      slot: 0, conn id: 2010, flow_id: 11, crypto map: l2tpoveripsec
      sa timing: remaining key lifetime (k/sec): (4194300/2514)
      IV size: 8 bytes
      replay detection support: N
   spi: 0x1FAB2B22(531311394)
      transform: esp-des ,
      in use settings ={Tunnel, }
      slot: 0, conn id: 2012, flow_id: 13, crypto map: l2tpoveripsec
      sa timing: remaining key lifetime (k/sec): (4194300/2554)
      IV size: 8 bytes
      replay detection support: N
   spi: 0x967E1FD7(2524848087)
      transform: esp-des ,
      in use settings ={Tunnel, }
      slot: 0, conn id: 2014, flow_id: 15, crypto map: l2tpoveripsec
      sa timing: remaining key lifetime (k/sec): (4159871/2552)
      IV size: 8 bytes
      replay detection support: N
  inbound ah sas:
  inbound pcp sas:
  outbound esp sas:
   spi: 0x19258116(421888278)
      transform: esp-des ,
      in use settings ={Tunnel, }
      slot: 0, conn id: 2003, flow_id: 4, crypto map: l2tpoveripsec
      sa timing: remaining key lifetime (k/sec): (4194298/2497)
      IV size: 8 bytes
      replay detection support: N
   spi: 0x19258118(421888280)
```

```
        transform: esp-des ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2007, flow_id: 8, crypto map: l2tpoveripsec
        sa timing: remaining key lifetime (k/sec): (4194298/2516)
        IV size: 8 bytes
        replay detection support: N
      spi: 0x19258119(421888281)
        transform: esp-des ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2009, flow_id: 10, crypto map: l2tpoveripsec
        sa timing: remaining key lifetime (k/sec): (4194298/2545)
        IV size: 8 bytes
        replay detection support: N
      spi: 0x1925811A(421888282)
        transform: esp-des ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2011, flow_id: 12, crypto map: l2tpoveripsec
        sa timing: remaining key lifetime (k/sec): (4194300/2514)
        IV size: 8 bytes
        replay detection support: N
      spi: 0x1925811B(421888283)
        transform: esp-des ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2013, flow_id: 14, crypto map: l2tpoveripsec
        sa timing: remaining key lifetime (k/sec): (4194300/2554)
        IV size: 8 bytes
        replay detection support: N
      spi: 0x1925811C(421888284)
        transform: esp-des ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2015, flow_id: 16, crypto map: l2tpoveripsec
        sa timing: remaining key lifetime (k/sec): (4192090/2550)
        IV size: 8 bytes
        replay detection support: N
     outbound ah sas:
     outbound pcp sas:
   local    ident (addr/mask/prot/port): (135.252.52.240/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (218.82.51.172/255.255.255.255/0/0)
   current_peer: 218.82.51.172
     PERMIT, flags={transport_parent,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
```

```
    #send errors 0, #recv errors 0
     local crypto endpt.: 135.252.52.240, remote crypto endpt.: 218.82.51.172
     path mtu 1500, ip mtu 1500
     current outbound spi: 0
     inbound esp sas:
     inbound ah sas:
     inbound pcp sas:
     outbound esp sas:
     outbound ah sas:
     outbound pcp sas:

Router#show vpdn session
L2TP Session Information Total tunnels 1 sessions 1
LocID RemID TunID Intf          Username          State   Last Chg Fastswitch
13    20    41009 Vi1           hiperl2tp         est     00:19:23 enabled
%No active L2F tunnels
%No active PPTP tunnels
%No active PPPoE tunnels

Router#show vpdn tunnel
L2TP Tunnel Information Total tunnels 1 sessions 1
LocID RemID Remote Name    State   Remote Address   Port   Sessions
41009 3111  4102367        est     218.82.51.172    1701   1
%No active L2F tunnels
%No active PPTP tunnels
%No active PPPoE tunnels
```

6.4.3 IPSec over L2TP ——HiPER 和 Cisco

本节主要介绍 IPSec over L2TP 的应用实例，在本例中，如图 6-34 所示，通过使用带有预共享密钥的 IKE 协议，采用“ 自动 ”密钥方式在上海分公司和北京总部之间采用 IPSec over L2TP 方式建立 VPN 隧道。上海使用 HiPER VPN 网关作为 L2TP 客户端，同时使其作为 IPSec 隧道的一端；北京使用 Cisco 2611 作为 L2TP 服务器，同时使其作为 IPSec 隧道的另一端。

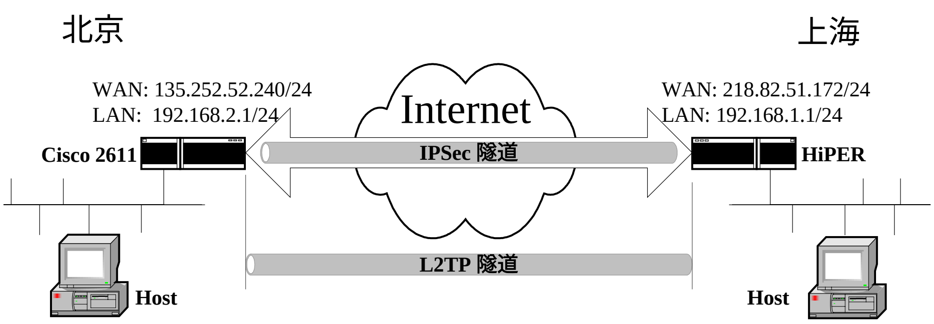


图 6-34 方案——IPSec over L2TP（HiPER 和 Cisco）

地址如下：

上海的 HiPER：

WAN 口： 218.82.51.172/24
静态网关：218.82.51.1/24
LAN 口： 192.168.1.1/24

北京的 Cisco 2611：

fastethernet0/1 口（外网接口）： 135.252.52.240/24
静态网关：135.252.52.1/24
fastethernet0/0 口（内网接口）： 192.168.2.1/24

1. 配置上海的 HiPER VPN 网关

提示：由于在 IPSec over L2TP 方式下，IPSec 加密的对象是内网用户数据包，故配置 IPSec 隧道时，“远端内网地址”和“本地内网地址”这两个参数均应配置成两端的内网地址；由于是先建立 L2TP 隧道，然后再建立 IPSec 隧道，本地 L2TP 的虚接口 IP 地址是 200.1.1.1/30，对方 L2TP 的虚接口 IP 地址是 200.1.1.2/30，因此，“远端网关地址（名）”设为 200.1.1.2；同时“本地绑定”应选择为 L2TP 隧道的“设置名”。

1) 配置 HiPER 成为 L2TP 客户端

在 ***VPN 配置—>PPTP 和 L2TP*** 中，选择“添加”选项，然后在配置参数项中依次输入以下内容（没有列出的参数项无需配置），再单击“保存”按钮。

“设置名”：l2tp_cisco
“业务类型”：拨出（客户端）
“用户名”：l2tpuser
“协议类型”：L2TP
“密码”：test
“确认密码”：test
“密码验证方式”：PAP
“远端内网 IP 地址”：192.168.2.0
“远端内网子网掩码”：255.255.255.0
“隧道服务器地址”：135.252.52.240
“对端虚接口 IP 地址”：200.1.1.2
“本地虚接口 IP 地址”：200.1.1.1
“虚接口子网掩码”：255.255.255.252

2) 配置 IPSec 隧道参数

在 ***VPN 配置—>IPSec*** 中，选择“添加”选项，然后在配置参数项中依次输入以下内容（没有列出的参数项无需配置）：

“设置名”：ipsec_l2tp
“设置方式”：自动
“自动方式”：网关到网关
“远端网关地址（名）”：200.1.1.2
“远端内网地址”：192.168.2.0
“远端内网掩码”：255.255.255.0
“本地绑定”：l2tp_cisco
“本地内网地址”：192.168.1.0
“本地内网掩码”：255.255.255. 0
“预共享密钥”（安全选项）：1234

“ 加密认证算法 1 ”（安全选项）：esp-des-sha

2. 配置 Cisco 2611 路由器

Cisco 2611 路由器只支持 CLI 方式，具体配置如下：

//配置 L2TP 隧道的用户名口令
username l2tpuser password 0 test
//激活 VPDN
vpdn enable
//配置 VPDN 组 1
vpdn-group 1
! Default L2TP VPDN group
accept-dialin
protocol l2tp
virtual-template 1
local name Router
lcp renegotiation always
no l2tp tunnel authentication
//配置第一阶段安全策略
crypto isakmp policy 1
authentication pre-share
group 2
crypto isakmp key cisco1234 address 200.1.1.1
crypto ipsec security-association lifetime seconds 28800
//配置第二阶段加密认证算法
crypto ipsec transform-set 1set esp-des esp-sha-hmac
//配置第二阶段安全策略
crypto map ipsecoverl2tp 10 ipsec-isakmp
set peer 200.1.1.1
set transform-set 1set
match address 124
//配置外网的接口地址
interface FastEthernet0/0
ip address 135.252.52.240 255.255.255.0
//配置内网的接口地址
interface FastEthernet0/1
ip address 192.168.2.1 255.255.255.0
//配置 L2TP 隧道参数
interface Virtual-Template1
ip address 200.1.1.2 255.255.255.252
peer default ip address pool l2tppool
ppp authentication pap
//将安全策略绑定到 L2TP 上
crypto map ipsecoverl2tp
//配置分配给 L2TP 隧道对端的虚接口 IP 地址
ip local pool l2tppool 200.1.1.1

ip classless

//配置路由

ip route 0.0.0.0 0.0.0.0 135.252.52.1

ip route 192.168.1.0 255.255.255.0 200.1.1.1

//配置 ACL 表，被安全策略引用

access-list 124 permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255

3. 查看状态

当双方配置完成后，上海的 HiPER 和北京的 Cisco 通过流量或者手工触发建立起 VPN 隧道。

1) 查看上海的 HiPER

对于上海的 HiPER 来说，可以在 ***VPN 配置—>PPTP 和 L2TP*** 中，查看 “ PPTP/L2TP 信息列表 ”，得到 L2TP 隧道的相关配置及状态信息，如表 6-45、表 6-46 所示；同时可以在 ***VPN 配置—>IPSec*** 中，查看 “ IPSec 信息列表 ”，得到 IPSec 隧道的相关配置及状态信息，如表 6-47、表 6-48、表 6-49 所示。

PPTP/L2TP 信息列表 1/17

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

	设置名	用户名	允许	会话状态	远端网关	远端内网地址	使用时间
☐	l2tp_cisco	l2tpuser	☑	已连接	135.252.52.240	192.168.2.0	00:00:22:05

表 6-45 L2TP over IPSec with Cisco — L2TP 信息列表

PPTP/L2TP 信息列表 1/17

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

使用时间	空闲时间	出流量	入流量	业务类型	协议类型	虚接口地址	是否加密
00:00:30:31	00:00:00:00	788860	788652	VPN拨出	L2TP	200.1.1.2	否

表 6-46 L2TP over IPSec with Cisco — L2TP 信息列表（续表 6-45）

从表 6-45 中，可以看到 “ 会话状态 ” 显示为 “ 已连接 ”，“ 出流量 ” 和 “ 入流量 ” 中均有数值显示；

从表 6-46 中，可以看到 “ 业务类型 ” 显示为 “ VPN 拨出 ”，协议类型显示为 “ L2TP ”，是否加密显示为 “ 否 ”。

IPSec 信息列表 1/16

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

	设置名	设置方式	允许	SA状态	远端网关	远端内网地址	外出加密包个数	进入解密包个数	本地绑定	本
☐	ipsec_l2tp	自动	☑	已建立	200.1.1.2	192.168.2.0	5768	5768	l2tp_cisco	

表 6-47 L2TP over IPSec with Cisco — IPSec 信息列表

IPSec 信息列表 1/16

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

本地内网地址	协商模式	加密认证算法	ESP外出SPI	ESP进入SPI	AH外出SPI	AH
192.168.1.0	主模式	esp-des-sha	0x86398c72(2251918450)	0x40f05ef0(1089494768)		

表 6-48 L2TP over IPSec with Cisco — IPSec 信息列表（续表 6-47）

IPSec 信息列表 1/16

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

出SPI	ESP进入SPI	AH外出SPI	AH进入SPI	生存时间(剩余)	筛选协议	筛选端口	UDP封装
2251918450)	0x40f05ef0(1089494768)			00:00:33:27	0	0	

表 6-49 L2TP over IPSec with Cisco — IPSec 信息列表（续表 6-48）

从表 6-47 中，可以看到“ 设置方式 ”显示为“ 自动 ”，“ SA 状态 ”显示为“ 已建立 ”， “ 外出加密包个数 ” 和 “ 进入解密包个数 ” 均有数值显示。

从表 6-48 中，可以看到 “ 本地绑定 ” 显示为 “ l2tp_cisco ”，“ 协商模式 ” 显示为 “ 主模式 ”，“ 加密认证算法 ” 显示为 “ esp-des-sha ”，“ ESP 外出 SPI ” 和 “ ESP 进入 SPI ” 显示为自动协商时得到的数值。

从表 6-49 中，可以看到 “ 生存时间（剩余）” 显示为 “ 00:00:33:27 ”，表示该 SA 的剩余有效时间为 33 分 27 秒。

2) 查看北京的 Cisco 2611

对于 Cisco 2611 路由器来说，可以通过命令 show crypto ipsec sa 、show vpdn session 及 show vpdn tunnel 查看 VPN 隧道配置及状态信息，具体信息如下：

```
Router#show crypto ipsec sa
interface: Virtual-Template1
    Crypto map tag: ipsecoverl2tp, local addr. 200.1.1.2
   local   ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   current_peer: 200.1.1.1
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 8264, #pkts encrypt: 8264, #pkts digest 8264
    #pkts decaps: 13498, #pkts decrypt: 13498, #pkts verify 13498
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0
     local crypto endpt.: 200.1.1.2, remote crypto endpt.: 200.1.1.1
     path mtu 1500, ip mtu 1500
     current outbound spi: 67302C6
     inbound esp sas:
      spi: 0xD0A2AB13(3500321555)
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: ipsecoverl2tp
        sa timing: remaining key lifetime (k/sec): (4177340/3112)
        IV size: 8 bytes
        replay detection support: Y
     inbound ah sas:
     inbound pcp sas:
     outbound esp sas:
      spi: 0x67302C6(108200646)
        transform: esp-des esp-sha-hmac ,
```

```
            in use settings ={Tunnel, }
            slot: 0, conn id: 2001, flow_id: 2, crypto map: ipsecoverl2tp
            sa timing: remaining key lifetime (k/sec): (4193392/3103)
            IV size: 8 bytes
            replay detection support: Y
      outbound ah sas:
      outbound pcp sas:
interface: Virtual-Access2
     Crypto map tag: ipsecoverl2tp, local addr. 200.1.1.2
   local   ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   current_peer: 200.1.1.1
      PERMIT, flags={origin_is_acl,}
     #pkts encaps: 8264, #pkts encrypt: 8264, #pkts digest 8264
     #pkts decaps: 13498, #pkts decrypt: 13498, #pkts verify 13498
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
     #send errors 0, #recv errors 0
      local crypto endpt.: 200.1.1.2, remote crypto endpt.: 200.1.1.1
      path mtu 1500, ip mtu 1500
      current outbound spi: 67302C6
      inbound esp sas:
       spi: 0x86398c72(3500321555)
            transform: esp-des esp-sha-hmac ,
            in use settings ={Tunnel, }
            slot: 0, conn id: 2000, flow_id: 1, crypto map: ipsecoverl2tp
            sa timing: remaining key lifetime (k/sec): (4177340/3103)
            IV size: 8 bytes
            replay detection support: Y
      inbound ah sas:
      inbound pcp sas:
      outbound esp sas:
       spi: 0x40f05ef0(108200646)
            transform: esp-des esp-sha-hmac ,
            in use settings ={Tunnel, }
            slot: 0, conn id: 2001, flow_id: 2, crypto map: ipsecoverl2tp
            sa timing: remaining key lifetime (k/sec): (4193392/3103)
            IV size: 8 bytes
            replay detection support: Y
      outbound ah sas:
      outbound pcp sas:

Router#show vpdn session
L2TP Session Information Total tunnels 1 sessions 1
LocID RemID TunID Intf            Username              State   Last Chg Fastswitch
```

13 3 14588 Vi2 l2tpuser est 00:08:40 enabled
%No active L2F tunnels
%No active PPTP tunnels
%No active PPPoE tunnels

Router#show vpdn tunnel
L2TP Tunnel Information Total tunnels 1 sessions 1
LocID RemID Remote Name State Remote Address Port Sessions
14588 3094 4102367 est 218.82.51.172 1024 1
%No active L2F tunnels
%No active PPTP tunnels
%No active PPPoE tunnels

6.4.4 多分支机构 IPSec

稍具规模的企业都不会只有一个办公场所，而是具有总部、分公司、办事处、工厂等多个业务点。解决位于不同地点的分支机构网络互联互通的一种比较好的方法，就是采用多分支机构 IPSec 的解决方案。

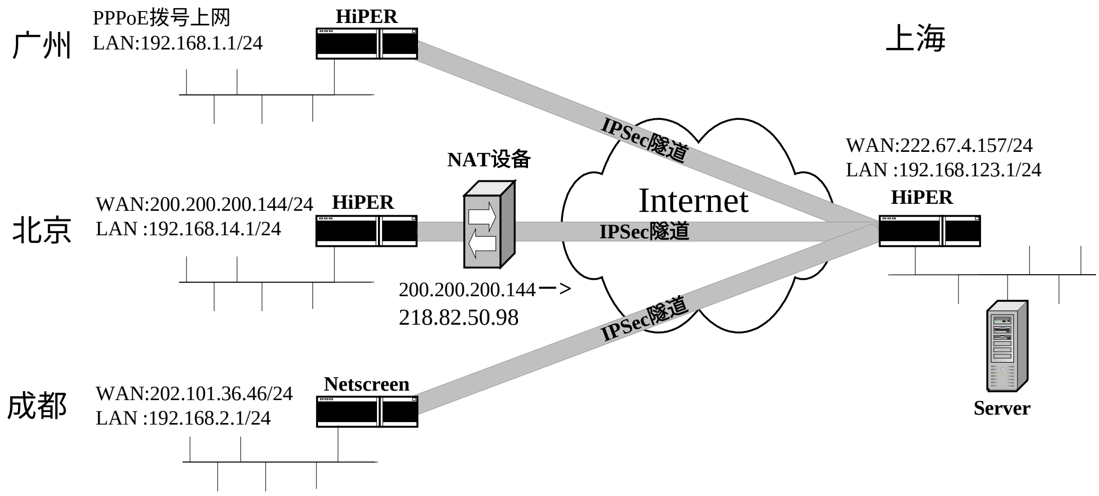


图 6-35 多分支机构 IPSec

本例中，如图 6-35 所示，假设一个企业的中心点位于上海，有位于广州、北京和成都的三个分支机构。广州、北京和成都的分支机构需要和上海总部通过公共网络建立安全的 IPSec 隧道。其中，上海、北京以及广州均使用 HiPER VPN 网关；成都使用 Netscreen。上海的 HiPER 通过 PPoE 获得固定地址上网，广州的 HiPER 采用 ADSL 的 PPPoE 拨号上网，成都的分支机构是 ISP 分配的固定的 IP 地址，而北京的分支机构则是通过一个 ISP 动态获取地址，而且该地址还经过 NAT 设备连接到公共网络。这三个分支机构和总部的 IPSec 连接都采用 ESP 的 3DES 加密，SHA-1 认证，预共享密钥是“ abccompanysecret ”。地址分配如下：

上海的 HiPER：

WAN 口地址：222.67.4.157/24

LAN 口地址：192.168.123.1/24

广州的 HiPER：

LAN 口地址：192.168.1.1/24

身份 ID：gz@abccompany.com

北京的 HiPER：

WAN 口地址：200.200.200.144/24

NAT 设备转化后地址：218.82.50.98/24

LAN 口地址：192.168.14.1/24

身份 ID：bj@abccompany.com

成都的 Netscreen

WAN 口地址：202.101.36.46/24

内网地址：172.16.10.1/24

1. 配置上海的 HiPER VPN 网关

1) 配置上海到广州的 IPSec 隧道参数

在 ***VPN 配置—>IPSec*** 中，选择 " 添加 " 选项，然后在配置参数项中依次输入以下内容（没有列出的参数项无需配置），再单击 " 保存 " 按钮。

" 设置名 "：sh_to_gz

" 设置方式 "：自动

" 自动方式 "：对方动态连接到本地

" 远端网关地址（名）"：0.0.0.0

" 远端内网地址 "：192.168.1.0

" 远端内网掩码 "：255.255.255.0

" 身份 ID "：gz@abccompany.com

" 身份类型 "：Email 地址

" 本地绑定 "：PPPoE

" 本地内网地址 "：192.168.123.0

" 本地内网掩码 "：255.255.255.0

" 预共享密钥 "（安全选项）：abccompanysecret

" 加密认证算法 1 "（安全选项）：esp-3des-sha

2) 配置上海到北京的 IPSec 隧道参数

" 设置名 "：sh_to_bj

" 设置方式 "：自动

" 自动方式 "：对方动态连接到本地

" 远端网关地址（名）"：0.0.0.0

" 远端内网地址 "：192.168.14.0

" 远端内网掩码 "：255.255.255.0

" 远端身份 ID "：bj@abccompany.com

" 身份类型 "：Email 地址

" 本地绑定 "：PPPoE

" 本地内网地址 "：192.168.123.0

" 本地内网掩码 "：255.255.255.0

" 预共享密钥 "（安全选项）：abccompanysecret

" 加密认证算法 1 "（安全选项）：esp-3des-sha

3) 配置上海到成都的 IPSec 隧道参数

" 设置名 "：sh_to_cd

" 设置方式 "：自动

“ 自动方式 ”：网关到网关
“ 远端网关地址（名）”：202.101.36.46
“ 远端内网地址 ”：192.168.2.0
“ 远端内网掩码 ”：255.255.255.0
“ 本地绑定 ”：PPPoE
“ 预共享密钥 ”（安全选项）：abccompanysecret
“ 加密认证算法 1 ”（安全选项）：esp-3des-sha

2. 配置广州的 HiPER VPN 网关

在 ***VPN 配置—>IPSec*** 中，选择“ 添加 ”选项，然后在配置参数项中依次输入以下内容（没有列出的参数项无需配置），再单击“ 保存 ”按钮。

“ 设置名 ”：gz_to_sh
“ 设置方式 ”：自动
“ 自动方式 ”：动态连接到网关
“ 远端网关地址（名）”：222.67.4.157
“ 远端内网地址 ”： 192.168.123.0
“ 远端内网掩码 ”：255.255.255.0
“ 本地绑定 ”：PPPoE
“ 本地内网地址 ”：192.168.1.0
“ 本地内网掩码 ”：255.255.255.0
“ 本地身份 ID ”：gz@abccompany.com
“ 本地身份类型 ”：Email 地址
“ 预共享密钥 ”（安全选项）：abccompanysecret
“ 加密认证算法 1 ”（安全选项）：esp-3des-sha
高级选项中：
“ 协商模式 ”：野蛮模式
“ DPD ”：选中
“ NAT 穿透 ”：选中

3. 配置北京的 HiPER VPN 网关

在 ***VPN 配置—>IPSec*** 中，选择“ 添加 ”选项，然后在配置参数项中依次输入以下内容（没有列出的参数项无需配置），再单击“ 保存 ”按钮。

“ 设置名 ”：bi_to_sh
“ 设置方式 ”：自动
“ 自动方式 ”：动态连接到网关
“ 远端网关地址（名）”：222.67.4.157
“ 远端内网地址 ”：192.168.123.0
“ 远端内网掩码 ”：255.255.255.0
“ 本地绑定 ”：WAN1（eth2）
“ 本地内网地址 ”：192.168.14.0
“ 本地内网掩码 ”：255.255.255.0
“ 本地身份 ID ”：bj@abccompany.com
“ 本地身份类型 ”：Email 地址
“ 预共享密钥 ”（安全选项）：abccompanysecret
“ 加密认证算法 1 ”（安全选项）：esp-3des-sha

4. 配置成都的 Netscreen

这里只给出基于 WEB UI 方式下配置 Netscreen 的方法。

配置接口－ 安全区段

1) 进入“Network”→“Interfaces”，单击“ethernet7 ”后的“Edit”超链接，输入以下内容，然后单击“OK”按钮。

“Zone Name”：Trust

“IP Address/Netmask”：192.168.2.1/24

2) 进入“Network”→“Interfaces”，单击“ethernet3”后的“Edit”超链接，输入以下内容，然后单击“OK”按钮。

“Zone Name”：Untrust

“IP Address/Netmask”：202.101.36.46/24

配置地址

3) 进入“Objects”→“Addresses”→“ List”，单击“New”按钮，再输入以下内容，然后单击“OK”按钮。

“Address Name”：Trust_LAN

“IP Address/Domain Name”：选中“IP/Netmask”

“IP/Netmask”：192.168.2.0/24

“Zone”：Trust

4) 进入“Objects”→“Addresses”→“ List”，单击“New”按钮，再输入以下内容，然后单击“OK”按钮。

“Address Name”：sh_office

“IP Address/Domain Name”：选中“IP/Netmask”

“IP/Netmask”：192.168.123.0/24

“Zone”：Untrust

配置 VPN

5) 进入“VPNs”→“AutoKey Advanced”→“Gateway”，单击“New”按钮，再输入以下内容。

“Gateway Name”：To_shanghai

“Security Level”：Custom

“Remote Gateway Type”：选中“Static IP Address”

“IP Address/Hostname”：222.67.4.157

“Preshared Key”：abccompanysecrect

“Outgoing Interface”：ethernet3

单击“Advanced”按钮，再输入以下高级设置参数：

“Security Level”：Custom

“Phase 1 Proposal”：pre-g2-3des-sha

“Mode（Initiator）”：Main

然后单击“Return”按钮，返回到上一页，再单击“OK”按钮。

6) 进入“VPNs”→“AutoKey IKE”，单击“New”按钮，再输入以下内容，然后单击“OK”按钮。

“VPN Name”：corp_branch

“Security Level”：Compatible

“Remote Gateway”：选中“Predefined”

“ Predefined ”：To_shanghai

配置路由

7) 进入 “ Network ” → “ Routing ” → “ Routing Table ”，选中 “ trust-vr ”，单击 “ New ” 按钮，再输入以下内容，然后单击 “ OK ” 按钮。

“ Network Address/Netmask ”：0.0.0.0/0
“ Gateway ”：选中
“ Interface ”：ethernet3（untrust）
“ Gateway IP Address ”：202.101.36.1

配置策略

8) 进入 “ Policies ”，“ From ” 选中 “ Trust ”，“ To ” 选中 “ Untrust ”，单击 “ New ” 按钮，再输入以下内容，然后单击 “ OK ” 按钮。

“ Source Address ”：选中 “ Address Book ”
“ Address Book ”：Trust_LAN
“ Destination Address ”：选中 “ Address Book ”
“ Address Book ”：sh_office
“ Service ”：ANY
“ Action ”：Tunnel
“ VPN Tunnel ”：corp_branch
“ Modify matching VPN policy ”：选中
“ Position at Top ”：选中

5. 查看状态

当各分支机构通过流量或者手工触发建立起 IPSec 隧道，对于上海、广州和北京的 HiPER 来说，可以在 ***VPN 配置—>IPSec*** 中，查看 “ IPSec 信息列表 ”，得到 IPSec 隧道的相关配置及状态信息。

1) 查看上海的 HiPER

如表 6-50、表 6-51、表 6-52 所示，为上海的 HiPER 的 IPSec 隧道的相关信息。

IPSec 信息列表 1/16

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

	设置名	设置方式	允许	SA状态	远端网关	远端内网地址	外出加密包个数	进入解密包个数	本地绑定
☐	sh_to_gz	自动	☑	已建立	50.50.50.6	192.168.1.1	5873	5873	PPPOE
☐	sh_to_bj	自动	☑	已建立	218.82.50.98	192.168.14.1	2517	2517	PPPOE
☐	sh_to_cd	自动	☑	已建立	202.101.36.46	192.168.2.1	2108	2108	PPPOE

表 6-50 多分支 IPSec 隧道（上海）— IPSec 信息列表

IPSec 信息列表 1/16

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

本地内网地址	协商模式	加密认证算法	ESP外出SPI	ESP进入SPI	AH外出SPI	AH进
192.168.123.1	野蛮模式	esp-3des-sha	0xcc5c33f9(3428594681)	0xc8ffa134(3372196148)		
192.168.123.1	野蛮模式	esp-3des-sha	0x5de8792a(1575516458)	0xbf4431cd(3208917453)		
192.168.123.1	主模式	esp-3des-sha	0x5de87924(1575516452)	0xbf4431c7(3208917447)		

表 6-51 多分支 IPSec 隧道（上海）— IPSec 信息列表（续表 6-50）

IPSec 信息列表 1/16

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

出SPI	ESP进入SPI	AH外出SPI	AH进入SPI	生存时间(剩余)	筛选协议	筛选端口	UDP封装
3428594681)	0xc8ffa134(3372196148)			00:00:22:00	0	0	
1575516458)	0xbf4431cd(3208917453)			00:00:51:22	0	0	
1575516452)	0xbf4431c7(3208917447)			00:00:47:49	0	0	

表 6-52 多分支 IPSec 隧道（上海）— IPSec 信息列表（续表 6-51）

从表 6-50 中，可以看到三条隧道的“设置方式”均显示为“自动”，“SA 状态”显示为“已建立”，“外出加密包个数”和“本地加密包个数”均有数值显示，本地绑定均显示为“PPPOE”，广州的 HiPER 当前获得的外网地址为“50.50.50.6”（对应于“设置名”为“sh_to_gz”的“远端网关”），北京的 HiPER 当前使用的外网地址为经 NAT 转化后获得的地址“218.82.50.98”（对应于“设置名”为“sh_to_bj”的“远端网关”）。

从表 6-51 中，可以看到隧道“sh_to_gz”和“sh_to_bj”的“协商模式”均为“野蛮模式”，而隧道“sh_to_cd”的“协商模式”为“主模式”，三条隧道的“加密认证算法”均为“esp-3des-sha”、“ESP 外出 SPI”和“ESP 进入 SPI”均显示为自动协商时得到的数值。

从表 6-52 中，可以看到三条隧道的“生存时间（剩余）”分别显示为“00:00:22:00”、“00:00:51:22”及“00:00:47:49”，表示对应 SA 的剩余有效时间分别为 22 分 00 秒、51 分 22 秒及 47 分 49 秒。

2) 查看广州的 HiPER

如表 6-53、表 6-54、表 6-55 所示，为广州的 HiPER 的 IPSec 隧道的相关信息。

IPSec 信息列表 1/16

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

	设置名	设置方式	允许	SA状态	远端网关	远端内网地址	外出加密包个数	进入解密包个数	本地绑定
☐	gz_to_sh	自动	☑	已建立	222.67.4.157	192.168.123.1	1603	1603	PPPOE

表 6-53 多分支 IPSec 隧道（广州）— IPSec 信息列表

IPSec 信息列表 1/16

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

本地内网地址	协商模式	加密认证算法	ESP外出SPI	ESP进入SPI	AH外出SPI	AH进
192.168.1.1	野蛮模式	esp-3des-sha	0xbf4431d0(3208917456)	0x5de8792d(1575516461)		

表 6-54 多分支 IPSec 隧道（广州）— IPSec 信息列表（续表 6-53）

IPSec 信息列表 1/16

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

出SPI	ESP进入SPI	AH外出SPI	AH进入SPI	生存时间(剩余)	筛选协议	筛选端口	UDP封装
3208917456)	0x5de8792d(1575516461)			00:00:52:15	0	0	

表 6-55 多分支 IPSec 隧道（广州）— IPSec 信息列表（续表 6-54）

从表 6-53 中，可以看到“设置方式”显示为“自动”，“SA 状态”显示为“已建立”，“外出加密包个数”和“进入解密包个数” 均有数值显示，“本地绑定”显示为“PPPOE”。

从表 6-54 中，可以看到“协商模式”显示为“野蛮模式”，“加密认证算法”显示为“esp-3des-sha”，“ESP 外出 SPI”和“ESP 进入 SPI”显示为自动协商时得到的数值。

从表 6-55 中，可以看到“生存时间（剩余）”显示为“00:00:52:15”，表示该 SA 的剩余有效时间为 52 分 15 秒。

3) 查看北京的 HiPER

如表 6-56、表 6-57、表 6-58 所示，为北京的 HiPER 的 IPSec 隧道的相关信息。

IPSec 信息列表 1/16

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

	设置名	设置方式	允许	SA状态	远端网关	远端内网地址	外出加密包个数	进入解密包个数	本地绑定
☐	bj_to_sh	自动	☑	已建立	222.67.4.157	192.168.123.1	1080	1080	eth2

表 6-56 多分支 IPSec 隧道（北京）— IPSec 信息列表

IPSec 信息列表 1/16

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

本地内网地址	协商模式	加密认证算法	ESP外出SPI	ESP进入SPI	AH外出SPI	AH进
192.168.14.1	野蛮模式	esp-3des-sha	0xbf4431d2(3208917458)	0x5de8792f(1575516463)		

表 6-57 多分支 IPSec 隧道（北京）— IPSec 信息列表（续表 6-56）

IPSec 信息列表 1/16

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

出SPI	ESP进入SPI	AH外出SPI	AH进入SPI	生存时间(剩余)	筛选协议	筛选端口	UDP封装
3208917458)	0x5de8792f(1575516463)			00:00:53:49	0	0	

表 6-58 多分支 IPSec 隧道（北京）— IPSec 信息列表（续表 6-57）

从表 6-56 中，可以看到“设置方式”显示为“自动”，“SA 状态”显示为“已建立”，“外出加密包个数”和“进入解密包个数” 均有数值显示，“本地绑定”显示为“eth2”。

从表 6-57 中，可以看到“协商模式”显示为“野蛮模式”，“加密认证算法”显示为“esp-3des-sha”，“ESP 外出 SPI”和“ESP 进入 SPI”显示为自动协商时得到的数值。

从表 6-58 中，可以看到“生存时间（剩余）”显示为“00:00:53:49”，表示该 SA 的剩余有效时间为 53 分 49 秒。

4) 查看成都的 Netscreen

对于成都的 Netscreen 来说，可以通过命令 get sa 查看 IPSec 隧道的配置及状态信息，具体信息如下所示：

```
ns208-> get sa
total configured sa: 4
HEX ID   S/D Gateway      Port  lgorithm       SPI        Life:sec kb Sta    PID vsys
00000025 0< 222.67.4.157   500 esp:3des/sha1 0x5de87924  1963 4095M A/-     25 0
00000025 0> 222.67.4.157   500 esp:3des/sha1 0xbf4431c7  1963 4095M A/-     24 0
```

附录一 十六进制 ASCII 码表

字符	回车	ESC	空格	!	"	#	$	%	&	’	(	)	*	+	,
ASCII 码	0D	1B	20	21	22	23	24	25	26	27	28	29	2A	2B	2C
字符	-	.	/	0	1	2	3	4	5	6	7	8	9	:	;
ASCII 码	2D	2E	2F	30	31	32	33	34	35	36	37	38	39	3A	3B
字符	<	=	>	?	@	A	B	C	D	E	F	G	H	I	J
ASCII 码	3C	3D	3E	3F	40	41	42	43	44	45	46	47	48	49	4A
字符	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
ASCII 码	4B	4C	4D	4E	4F	50	51	52	53	54	55	56	57	58	59
字符	Z	[	\	]	^	-	a	b	c	d	e	f	g	h	i
ASCII 码	5A	5B	5C	5D	5E	5F	61	62	63	64	65	66	67	68	69
字符	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
ASCII 码	6A	6B	6C	6D	6E	6F	70	71	72	73	74	75	76	77	78
字符	y	z	{	|	}	~									
ASCII 码	79	7A	7B	7C	7D	7E									

附录二　图索引

附录三　表索引